INHIBIDOR DE SEÑALES LTE MEDIANTE PLATAFORMA SOFTWARE DEFINED RADIO

TRABAJO FIN DE GRADO

ALUMNO: JACOBO CALVO MORENO
TUTOR: VÍCTOR PEDRO GIL JIMÉNEZ
TITULACIÓN: GRADO EN INGENIERÍA EN TECNOLOGÍAS DE TELECOMUNICACIÓN
FECHA: 22 DE JUNIO DE 2015

Índice de contenidos

Índice de tablas

Índice de ilustraciones

Acrónimos

- MSK: Minimum Shift Keying
- GMSK: Gaussian MSK
- GSM: Global System for Mobile
- PSK: Phase Shift Keying
- EDGE: Enhanced Data Rates for GSM Evolution
- QAM: Quadrature Amplitude Modulation
- UMTS: Universal Mobile Telecommunications System
- LTE: Long Term Evolution
- IFFT: Inverse Fast Fourier Transform
- BPSK: Binary PSK
- QPSK: Quadrature PSK
- FDMA: Frequency Division Multiple Access
- TDMA: Time Division Multiple Access
- SDMA: Space Division Multiple Access
- CDMA: Code Division Multiple Access
- HSDPA: High Speed Downlink Packet Access
- HSUPA: High Speed Uplink Packet Access
- HSPA: High Speed Packet Access
- LTE: Long Term Evolution
- OFDMA: Orthogonal FDMA
- UL: Uplink
- DL: Downlink
- DL-RS: Downlink Reference Signal
- SCH: Synchronization Channel
- PCFICH: Physical Control Format Indicator Channel
- PBCH: Physical Broadcast Channel
- PHICH: Physical HARQ Indicator Channel
- PDSCH: Physical Downlink Shared Channel
- PUSCH: Physical Uplink Shared Channel
- PDCCH: Physical Downlink Control Channel
- PUCCH: Physical Uplink Control Channel
- PMCH: Physical Multicast Channel
- MBSFN: Multicast Broadcast Single Frequency Network
- FDD: Frequency Division Duplexing
- TDD: Time Division Duplexing
- RACH: Random Access Channel
- SCCPCH: Secondary Common Control Physical Channel
- TCFI: Transport Format Combination Indicator

Summary

This Bachelor Thesis consists in the realization of an application trough Software Defined Radio that inhibits the signal of LTE mobile communications system. The fact of working with mobile communications supposes a motivation in professional and academic aspects, because they are a leading economic activity in our society and it is the branch of the Bachelor Degree in Telecommunication Technologies I like the most.

Inhibitors have multitude of utilities, even though its uses are limited within a legal framework to the areas related to public security, national defence, State security and activities related to Criminal Law.

The goal will be to implement an application which can leave a specific operator's terminals (but available for all of them) without LTE signal inside the radius of inhibition. Also it will be the goal to minimize the relation in the user equipment between inhibitor's power and eNodeB's power, what means maximize the inhibition radius and minimize the inhibitor transmission power.

The duration of this Bachelor Thesis will be 145 days, divided in different activities as the following table shows:

Task	Introduction	Duration (days)
Bachelor Thesis adjudication	0	1
Information search	1	3
Theoretical study	4	20
LabVIEW learning	24	4
Application development	28	30
Testing	58	20
Improvements	78	10
Writing report	88	30
Reviewing report	118	15
Handing over report	133	1
Presentation preparation	134	10
Work defence	144	1

Table 1/Bachelor Thesis's schedule

The corresponding Gantt's diagram is as follows:

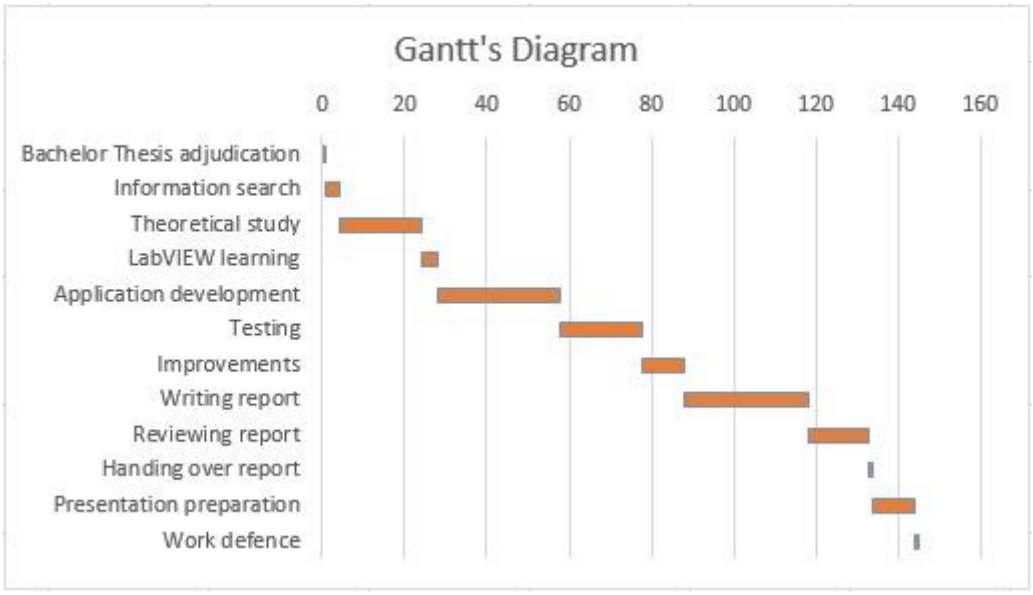


Figure 1/Gantt's diagram

At present, LTE system has different vulnerabilities, so it is possible to inhibit communication interfering any of its channels as are following: PDSCH, PUSCH, PCFICH, PUCCH, PBCH. To inhibit the communication, we have chosen to transmit random synchronization signals (PSS y SSS) as it is explained in [5].

To produce our attack it is necessary to transmit the frame shape of LTE downlink and to map synchronization signals correctly in the frame. A frame has a duration of 10 milliseconds and is divided in 10 subframes. Each subframe is divided at the same time in 2 slots. The frame structure that uses LTE using FDD is the following:

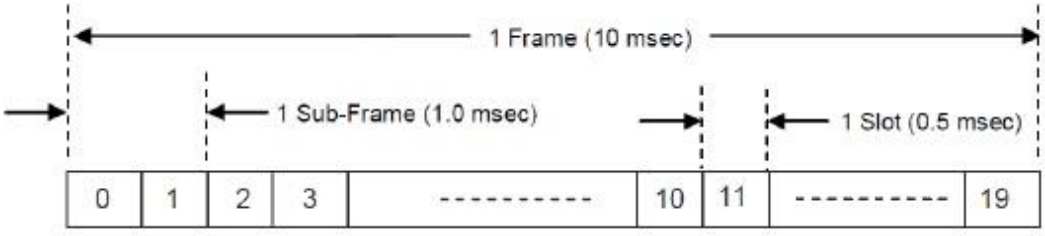


Figure 2/ Frame structure

Each frame is composed by 20 slots of 0,5 milliseconds each one. The slot structure depends on the size of the cyclic prefix, as it can be normal or extended. Cyclic prefix is used as guard band between OFDMA symbols to it doesn't lose orthogonality between them. In our case we will use a normal cyclic prefix, because is the most used.

The slot structure for a normal cyclic prefix is the following:

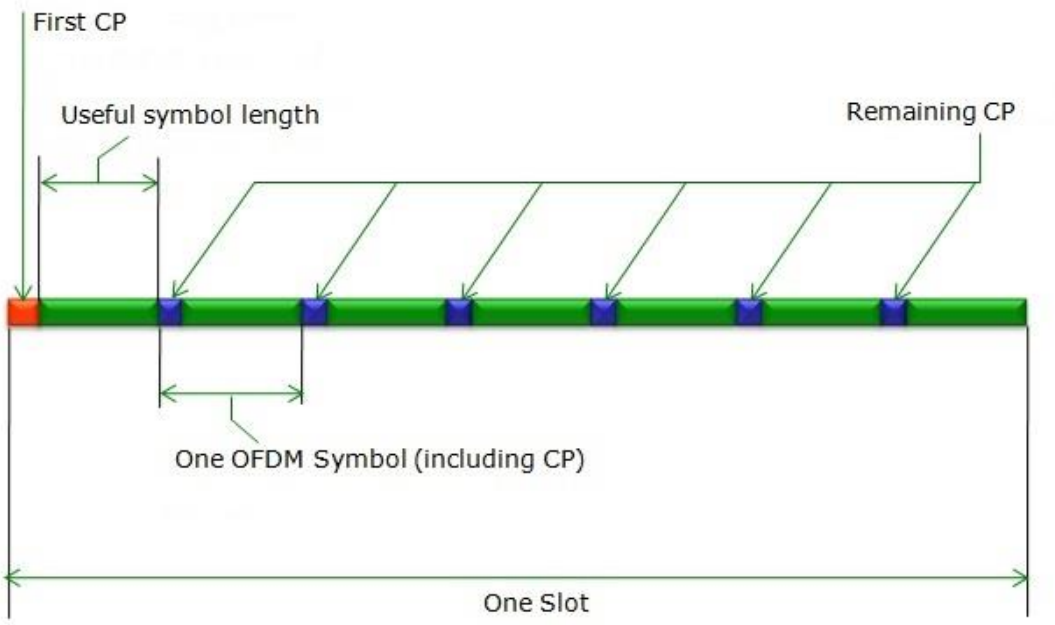


Figure 3/Slot structure

As it is showed in the image, a slot will contain 7 OFDMA symbols, and each symbol will be preceded by a cyclic prefix. The channels are mapped in the frame as the following image shows:

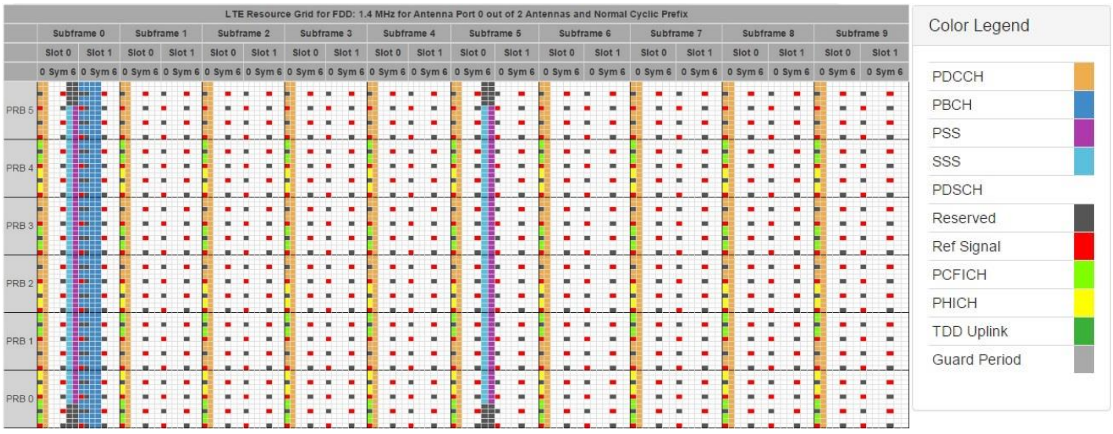


Figure 4/Frame with channels and physic signals

As shown, PSS will be transmitted in the seventh symbol of the slots 1 and 11, and SSS in the sixth symbol of the slots 1 and 11, although before the mapping it will be necessary to make IFFT for both signals.

Both PSS and SSS have a length of 62 elements. They will be filled out with 33 zeros on each side until they have a size of 128 so it is possible to carry out IFFT of size 128.

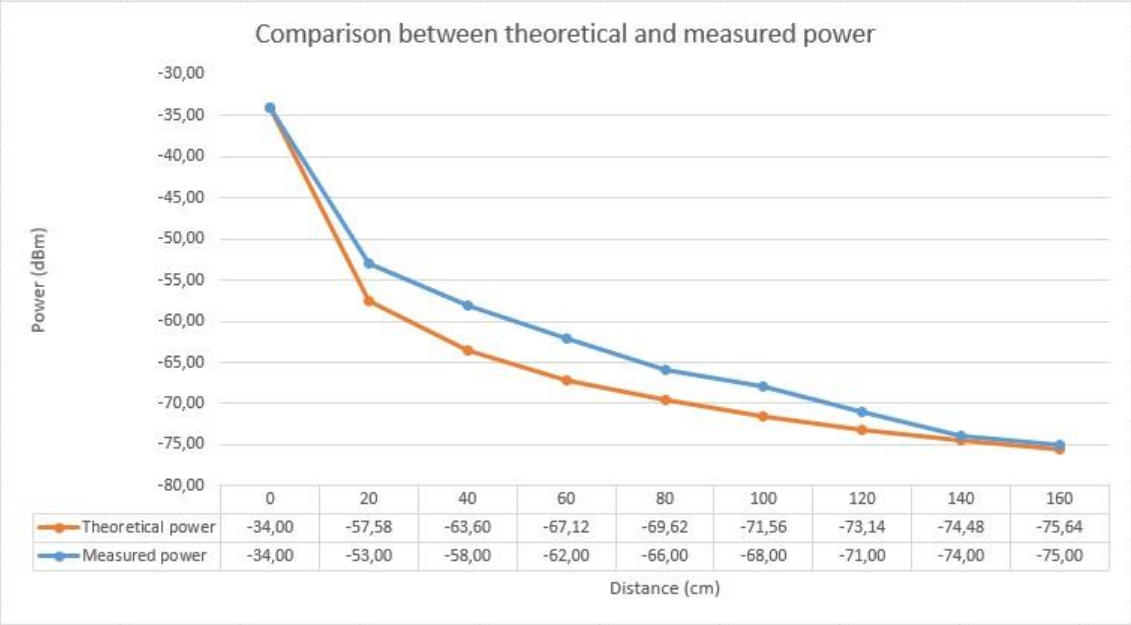
Before the realization of the IFFT it will be necessary to replace the 64 first elements by the seconds, and vice versa. Once it has been carried out, the signals will be mapped and the frame will be transmitted continuously. The other elements of the frame will be modulated zeros.

After carrying out some tests with different terminals and for all the operators, we can say that our inhibitor has been a success, because we get inhibit in every case and with optimum results.

Our device has a transmission power[1] on the edge of the antenna of -34 dBm. The power transmitted by the device for different distances has been measured and compared to the theoretical power that should arrive to those distances keeping in mind the basic losses of propagation:

$$L_{bf}(dB) = 32{,}45 + 20\log f(MHz) + 20\log d(km)$$

The result is the following:



	0	20	40	60	80	100	120	140	160
Theoretical power	-34,00	-57,58	-63,60	-67,12	-69,62	-71,56	-73,14	-74,48	-75,64
Measured power	-34,00	-53,00	-58,00	-62,00	-66,00	-68,00	-71,00	-74,00	-75,00

Figure 5/ Comparison between theoretical and measured power.

As the image shows, measured transmitted power is very similar to theoretical. The difference of power, that can reach 5 dB, can be because of the interferences produced in the room where this measure was carried out.

The power received by Vodafone are -61 dBm. With this operator we obtained a radius of 22cm. The power that we measured in this point is approximately[2] -53 dBm, and the Vodafone one is -61 dBm. Therefore can be said that, to inhibit, we need to interfere the original signal in more than 8dB.

[1] All power measurements are made for a bandwidth of 1.4 MHz. For the inhibitor's transmission power measurements 1800 MHz was used as frequency carrier.
[2] We use the power measured at a distance of 20 cm because it is the closest to 22 cm.

However, if the same appreciation is done to the theoretical power[3] value in that point, -58 dBm, that is more exact because it has no interferences, can be determined that is only necessary to interfere the signal in more than 2,6 dB.

This is a very positive result with regard to the efficiency of our device, being that currently the inhibitors need to interfere the original signal in more than 30 dB.

For the realization of this Bachelor Thesis we have made the following budget[4]:

Material	Cost
LabVIEW Student Edition licence	0 €
NI USRP 2920	3.000 €
Equipment with hardware VXI Agilent and software VSA	5.000 €
Microsoft Office 365 Licence	35 €
Computer ASUS A52J version K52JU	600 €
Student work	14.400 €
Professor work	3.600 €
Indirect costs	500 €
TOTAL	27.135 €

Table 2/Bachelor Thesis's budget

[3] The exact value for a distance of 22 cm has been calculated with the basic propagation losses equation taking -34 dBm as reference as it's measured at the edge of the antenna.
[4] Taxes included.

1. Introduction

1.1 Motivation and goals

Nowadays communications are the base of the society we live. Thanks to them we can know what is happening around the world immediately or establish easily a conversation between two places in the world, between two or more people.

Mobile communications are the most used in this moment, not only because they let voice traffic, also because it is possible to log in to Internet at high speed. Although they are a benefit for society, a bad use of them can be quite damaging. This is why there are situations where it is necessary inhibit this communication and for that we need inhibitors.

These devices emit radio waves in the same frequencies that the ones used for mobile communications but at higher power, getting then interfering in the link and prevent communication.

It is used in multiple areas of society:

- Military and civil.
- Security and restricted use.
- Classrooms, meeting, congresses, churches, penitentiaries, anti-terrorism protection, etc.

The Communication Group of the University Carlos III of Madrid has developed a patent[5] about an inhibitor for 3G or 4G that gets a higher efficiency than the used currently. My work will be to develop this for LTE through Software Defined Radio, using LabVIEW as work tool and Ni USRP 2920 hardware.

Carrying out this project will help me study mobile systems, mainly LTE, understanding them better so that they can help me in my professional future. This will be the main goal of this work because I would like to work in the investigation of the mobile systems in a future.

The goal of this Bachelor Thesis is to develop an application that inhibits the LTE signal in the mobile. For that, we will implement an application which can leave a specific operator's terminals (but available for all of them) without LTE signal inside the radius of inhibition. Also it will be the goal to minimize the relation in the user equipment between inhibitor's power and eNodeB's power, what means maximize the inhibition radius and minimize the inhibitor transmission power. We will use the hardware NI USRP 2920, that will let us transmit and the software LabVIEW, which we will program for our need.

[5] http://www.google.es/patents/WO2014041225A1?cl=es&hl=es

It is also necessary to design the signal that we will transmit to interfere with the real signal. For this, we will use the patent and the core subjects of the Bachelor's Degree in Telecommunication Technologies.

1.2 Report Structure

The report has six main chapters:

- 1. Introduction. In which are developed some fundamental aspects like motivations and goals for this work, report structure, planning and regulations of the device made.
- 2. Art state. Present inhibitors are compared with the developed proposition.
- 3. Mobil Phones. In this chapter, we review the Mobile Phone Technologies that have existed until LTE to understand better this new voice and data mobile communication system.
- 4. Theoretical aspects of LTE. All the necessary knowledge to develop our device will be exposed in this chapter.
- 5. Application description. How application has been developed from the theoretical point of view and the graphical interface.
- 6. Conclusions. In this final chapter are exposed the results of the testing period and the budget involved in this Bachelor Thesis.

1.3 Bachelor Thesis's schedule

The next table shows the Bachelor Thesis's schedule followed throughout this project:

Task	Introduction	Duration (days)
Bachelor Thesis adjudication	0	1
Information search	1	3
Theoretical study	4	20
LabVIEW learning	24	4
Application development	28	30
Testing	58	20
Improvements	78	10
Writing report	88	30
Reviewing report	118	15
Handing over report	133	1
Presentation preparation	134	10
Work defence	144	1

Table 3/Bachelor Thesis's schedule

As it is showed, the total duration of this project is 145 days. Corresponding to Gantt's diagram:

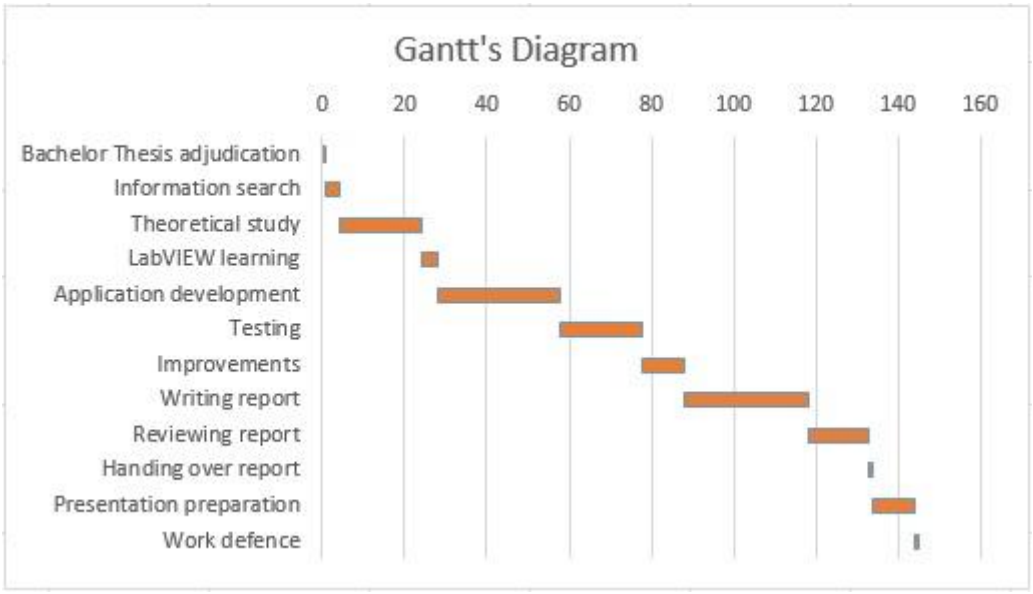


Figure 6/Gantt's diagram

1.4 Regulatory framework

Although the sector of telecommunication and information technologies is amply regulated, there is not a specific law about frequency inhibitors. For that, the General Commissioner of Public Safety of the National Police made a report[6] in February 16th 2010 to establish a regulatory framework not binding about devices.

This report is based in the applicable regulations to this kind of issues, which it quotes here:

- Directive of the European Community 99/05/CE.
- Royal Decree 1890/2000 of November 20th by which it is approved the process for the evaluation for conformity of telecommunications equipment.
- Report of the State Secretary of Technologies of December 28th, 2004.
- III title of the Law 32/2003 of November 3rd, General Telecommunication.
- Commission decision of April 6th, 2000 related to establishing the initial classification of electromagnetic equipment and mobile equipment of telecommunication and associated identifiers.
- Commission decision of July 26th 2002 by which it was created a Politic Group about electromagnetic spectrum.
- Decision nº 676/2002/CE of the European Parliament and the Council about a regulatory framework of the electromagnetic spectrum politics of the European Community.

[6]http://www.policia.es/org_central/seguridad_ciudadana/unidad_central_segur_pri/i_reservada/2010/2010_009.pdf

TCAM (Telecommunications Conformity Assessment and Market Surveillance Committee) of European Commission has agreed that using these devices is not allowed, neither the sell, and may punish to the ones who break the regulations with fines between 500.000 and 20 million Euros.

Further, frequency inhibitors must comply Directive 99/05/CE because of the use of electromagnetic spectrum.

However, activities related to public security, national defence, state security and State activities related to Criminal Law are allowed to use it. This activities are exempt of the application of this regulation.

2. Estado del arte

Un inhibidor convencional, en el sector de las Telecomunicaciones, se define como "un dispositivo electrónico que impide o dificulta las transmisiones radioeléctricas en un determinado rango de frecuencias mediante la emisión de una señal de mayor potencia que la del emisor que quiere transmitir"[7] según se expone en [5].

Actualmente existen inhibidores de frecuencia para los sistemas en uso (2G, 3G y 4G) que inhabilitan las frecuencias que utilizan los terminales para comunicarse con las estaciones base, impidiendo así la recepción y el envío de llamadas y datos en los teléfonos móviles cubiertos por el radio de acción del inhibidor.

Su uso principalmente es por motivos de seguridad en determinados lugares donde se requiere imposibilitar la comunicación en ambos sentidos por diversos motivos como el espionaje o conversaciones no autorizadas. También se utilizan en los vehículos oficiales o con riesgo de algún posible ataque.

Estos inhibidores de frecuencia se fundamentan en la transmisión de ruido en la banda de frecuencias del sistema que desean inhibir (como el sistema que plantea en [19]). Este método es efectivo en los sistemas de segunda generación como GSM, ya que utilizan banda estrecha, pero en los sistemas de tercera y cuarta generación que hacen uso de espectro ensanchado son muy ineficientes.

Un ejemplo de este caso es:

- Diseño e implementación de prototipo inhibidor de señales de celular para un salón de clases [15]: se diseña un dispositivo que emite una señal de onda triangular de 4 Vpp en todo el ancho de banda de cada frecuencia que se desee inhibir. Se consigue una potencia real de salida promedio de 25 dBm en la banda de 850 MHz y de 20 dBm en la de 1900 MHz.

UMTS y LTE, por su propia naturaleza (utilizan WCDMA y OFDMA respectivamente), son muy robustos frente a las interferencias. Por ello es necesario transmitir mucha más potencia que en el caso de GSM para conseguir inhibir las señales, y en ocasiones, hasta superar los límites marcados por la legislación sobre emisiones radioeléctricas.

Otras alternativas son las planteadas en las siguientes patentes:

- "US 2009/0227199 A1": introduce una señal de potencia elevada que interfiere directamente en el canal de acceso aleatorio (RACH).

[7] http://www.google.es/patents/WO2014041225A1?cl=es&hl=es

- "US 2011/0086590 A1": el dispositivo recibe una señal de la estación base para iniciar una sesión de comunicación, pudiendo así sincronizarse con el canal físico secundario (CCPCH) y alterar la indicación de la combinación del formato de transporte (TCFI). Con el TCFI alterado, genera copias de la señal, se multiplexan y las envía al terminal desplazadas en tiempo como señal de interferencia, logrando así que este no pueda determinar la información transmitida por la estación base.

También existen múltiples tipos de amenazas posibles al sistema LTE interfiriendo a determinados canales como se explica en [16]:

- PDSCH y PUSCH: estos dos canales se utilizan para transmitir la información de usuario del eNodeB al terminal y viceversa respectivamente. Utilizan una modulación adaptativa dependiendo de la calidad del canal, que pueden ser 64QAM, 16QAM y QPSK. Es necesario como mínimo una tasa de codificación de 0.076. Si interferimos estos dos canales forzándolos a utilizar una QPSK y a usar una tasa de codificación por debajo del mínimo, provocaremos un gran número de retransmisiones consiguiendo así inhabilitar la comunicación.
- PCFICH: este canal contiene la situación en el dominio del tiempo y de la frecuencia del PDCCH, por lo que si interferimos el PCFICH impidiendo su decodificación, sería imposible decodificar el PDCCH, el cual es fundamental para el funcionamiento del sistema LTE. Para interferir el PCFICH será necesario transmitir por encima suya (aparece en un símbolo por subtrama y ocupa 16 subportadoras) pero no tiene una ubicación estática, por lo que para determinar la ubicación exacta es necesario conocer el ID de la célula. El ID se obtiene a partir de la PSS y la SSS, así que será necesario sincronizarse con el eNodeB para conseguirlo (obliga a sincronizarse con cada célula dentro de la cual queramos inhibir).
- PUCCH: este canal contiene información de control necesaria para la comunicación que envía el terminal al eNodeB. Está situado en los bordes del símbolo, por lo que para interferirlo no basta con conocer la frecuencia de portadora, también será necesario el ancho de banda. Para un ancho de banda de 10 MHz se deben interferir 192 subportadoras aproximadamente, lo que supone un 25% - 30 % del total.
- PBCH: después de la sincronización con la PSS y la SSS el terminal recibe el Master Information Block (MIB), información esencial para el acceso inicial a la célula. El MIB se transporta en el PBCH, por lo que interfiriendo sobre este canal el terminal no podría decodificar el MIB y por ende conectarse a la célula. Sería necesario interferir en las 72 subportadoras centrales, ya que es donde se transmite el PBCH, específicamente en la primera subtrama de cada trama.

- PSS: la detección de esta señal es el primer paso para conectarse a una célula. Es por ello que está diseñada para ser detectada a altos niveles de interferencia, por lo que un ataque de este tipo requeriría demasiada potencia. Un método más efectivo sería suplantar la identidad del eNodeB transmitiendo las tres posibles PSS, ya que sería suficiente con transmitir unos 3 dB por encima de la señal real para que el terminal decidiese sincronizarse al inhibidor. Aunque este ataque es muy eficiente en cuanto a potencia, LTE está protegido ante él: Una vez el terminal se ha sincronizado con la PSS, intenta hacerlo con la SSS, y al no existir, cataloga la señal como "falsa" conectándose a otra (la real) aunque su potencia sea más baja.

Existe un amplio abanico de inhibidores a la venta. Estos son algunos ejemplos [17]:

- TX101E: se trata de un inhibidor portátil de red móvil 2G, 3G y 4G. Tiene un alcance de entre 5 y 15 metros emitiendo una potencia de 2 W con sus 4 antenas. Su precio es de 310 €. (http://www.projammers.com/es/home/tx121e-inhibidor-portatil.html)
- TX101A6: se trata de un inhibidor de red móvil 2G, 3G, 4G y WiFi. Tiene un alcance de entre 10 y 40 metros emitiendo una potencia de 15 W con sus 6 antenas. Su precio es de 530 €. (http://www.projammers.com/es/home/tx101a6-inhibidor-de-frecuencia.html)
- TX107DJ: se trata de un inhibidor de red móvil 2G, 3G y 4G. Tiene un alcance de hasta 50 metros emitiendo una potencia de 15 W con sus 7 antenas. Además está camuflado bajo un cuadro, tiene un aspecto discreto. Su precio es de 2200 €. (http://www.projammers.com/es/home/tx107dj-inhibidor-de-frecuencias.html)
- TX101K6: se trata de un inhibidor de red móvil 2G, 3G, 4G y WiFi. Tiene un alcance de hasta 200 metros emitiendo una potencia de 65 W con sus 6 antenas. Su precio es de 4500 €. (http://www.projammers.com/es/home/tx101k6-inhibidor-de-frecuencias.html)

3. Telefonía móvil

3.1 Introducción

Para remontarnos al inicio de las comunicaciones móviles tal y como las conocemos hoy en día deberíamos hacernos una pregunta: ¿cómo surgió la idea de usar la radio para la comunicación móvil? Esta idea surgió de los experimentos realizados por Guglielmo Marconi sobre transmisión a larga distancia, en los que instalaba un sistema de "radio móvil" sobre tranvías. En los años 20 la policía de Detroit comenzó a usar el primer servicio de telefonía móvil, que tan sólo consistía en el envío de mensajes de aviso, pero desde entonces han aparecido gran cantidad de sistemas.

A lo largo de este proceso se han logrado avances tecnológicos y teóricos muy importantes:

- El desarrollo del transistor (inventado en los laboratorios Bell a finales de los años 40) y los circuitos integrados han permitido la revolución de la microelectrónica, es decir, la reducción del tamaño y precio de muchos dispositivos consiguiendo así su extensión y popularización.

- La modulación en frecuencia permitió conseguir un sistema mucho más robusto frente a las interferencias, además de los códigos de protección contra errores y la división por código.

- El sistema celular: consiste en reutilizar las frecuencias disponibles entre un número de estaciones base determinado coordinadas entre sí. Esto permite que el sistema pueda tener toda la extensión y capacidad requeridas con sólo hacer las células más pequeñas. Además, el handover permite el cambio de estación base sin afectar a la comunicación y el roaming disponer de cobertura en otro país haciendo uso de otro operador, consiguiendo una mayor libertad de movimiento para los usuarios.

En paralelo a estos desarrollos, los servicios se han ido extendiendo al grueso de la población debido a la mejora de la calidad y a la reducción de precios, ya que inicialmente se diseñaron para usos específicos como el militar.

En la siguiente tabla podemos comprobar cómo ha aumentado el número de líneas móviles en España.

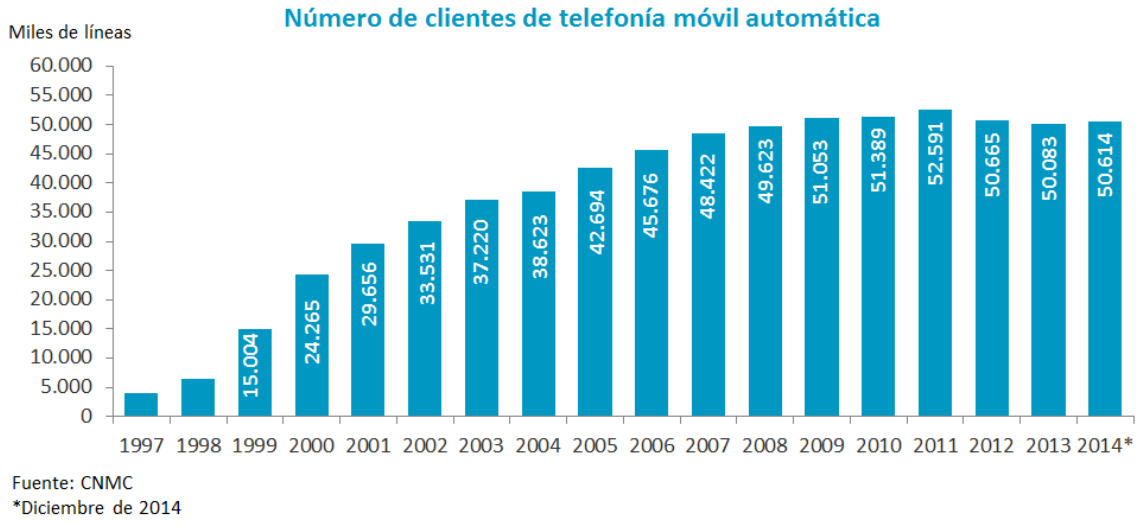


Ilustración 7/Número de líneas móviles en España[8]

Si prestamos un poco de atención a los datos más recientes podemos comprobar cómo el número de líneas ha superado el número de habitantes. Efectivamente, la penetración de la telefonía móvil es superior al 100%.

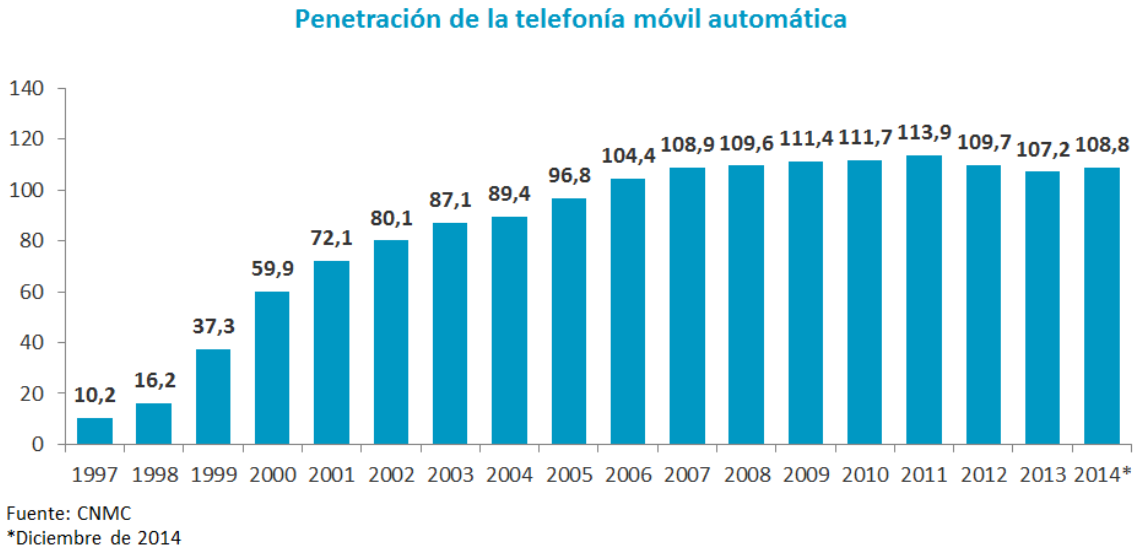


Ilustración 8/Penetración de la telefonía móvil en España[9]

8 http://www.ontsi.red.es/ontsi/es/indicador/evoluci%C3%B3n-del-n%C3%BAmero-de-clientes-de-telefon%C3%ADa-m%C3%B3vil-en-espa%C3%B1a

9 http://www.ontsi.red.es/ontsi/es/indicador/evoluci%C3%B3n-del-n%C3%BAmero-de-clientes-de-telefon%C3%ADa-m%C3%B3vil-en-espa%C3%B1a

3.2 Modulaciones utilizadas en telefonía móvil

Como hemos comentado en el apartado anterior, uno de los principales avances tecnológicos que han hecho posible la telefonía móvil tal y como la conocemos ahora es la modulación en frecuencia.

Los primeros sistemas de telefonía móvil eran analógicos (1G) y usaban una modulación en fase (analógica), cuya portadora se representa de la siguiente forma:

$$y(t) = A\cos[\omega_c\, t + \ \varphi(t)]$$

Donde el ángulo de fase $\varphi(t)$ varía de forma proporcional a $x(t)$, la señal de información.

Conforme crecía el número de usuarios fue necesario aumentar el número de líneas conectadas a un transmisor, por lo que se desarrollaron las técnicas de acceso múltiple, siendo necesario el uso de modulaciones digitales. Entre las más utilizadas se encuentran:

- GMSK: Es una variación de la modulación MSK añadiéndole un pre filtrado gaussiano y se usa en GSM y GPRS. Envía un bit por símbolo, representando cada bit una dirección respecto a la posición del símbolo anterior.

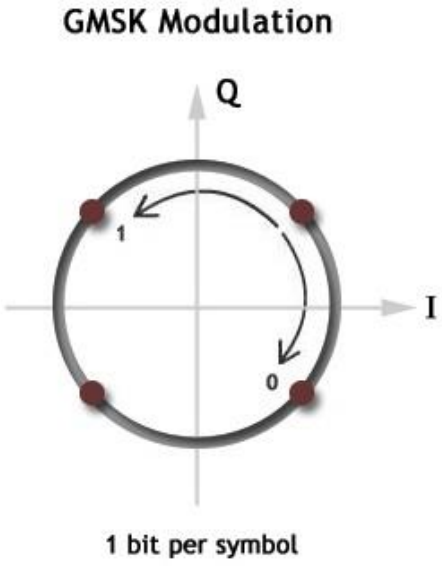


Ilustración 9/Modulación GMSK[10]

[10] http://mobilorus.blogspot.com.es/2013/03/which-modulation-types-are-being-used.html

- 8PSK: Es una variación de la PSK y se usa en EDGE. Consiste en asociar un símbolo a cada conjunto de 3 bits, consiguiendo 8 combinaciones diferentes.

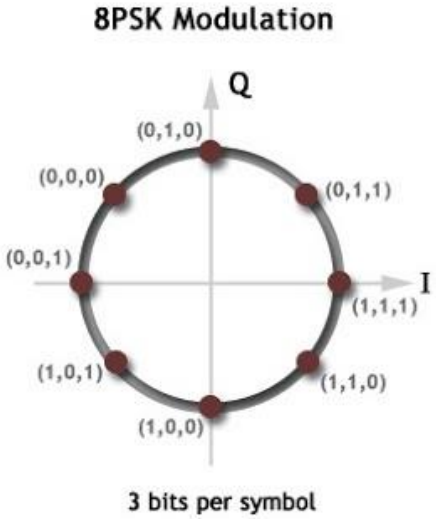


Ilustración 10/Modulación 8PSK[11]

- QAM: Se utiliza en UMTS y LTE. Un ejemplo sería la 64QAM, que consiste en asignar 6 bits a cada símbolo, consiguiendo 64 combinaciones diferentes.

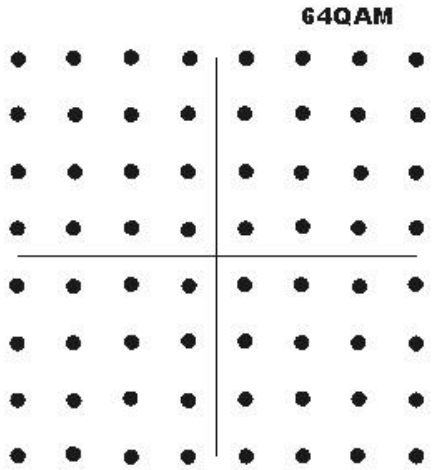


Ilustración 11/Modulación 64QAM[12]

[11] http://mobilorus.blogspot.com.es/2013/03/which-modulation-types-are-being-used.html

[12] http://mobilorus.blogspot.com.es/2013/03/which-modulation-types-are-being-used.html

En LTE se usan diferentes tipos de modulaciones muy similares a la anterior.

Modulación	Bits por símbolo
BPSK	1
QPSK	2
16QAM	4
64QAM	6

Tabla 4/Modulaciones LTE

3.3 Acceso múltiple

Otro de los avances tecnológicos mencionados es el sistema celular, que además de reutilizar las frecuencias por celdas requiere las técnicas de acceso múltiple adecuadas para poder dar servicio a un gran número de líneas conectadas a una sola estación base.

"Se denomina canal físico a la facilidad concedida a un usuario mediante la cual éste puede acceder al sistema. Las técnicas de multiacceso son procedimientos de asignación de canales físicos a las estaciones." [13]

Los métodos básicos de acceso múltiple son los siguientes:

- FDMA, acceso múltiple por división de frecuencia.
- TDMA, acceso múltiple por división de tiempo.
- CDMA, acceso múltiple por división de código.

3.3.1 FDMA

FDMA se basa en la separación de frecuencias del volumen espectral; el ancho de banda se divide en radiocanales separados por una banda de paso Δf para no interferirse entre sí. Cada uno de estos radiocanales estará asignado a un usuario en la interfaz radio y será del tipo un solo canal por portadora (SCPC). Los usuarios de una estación base usarán sólo su radiocanal gracias al uso de un filtro sintonizable.

Además, gracias al uso del sistema celular, las estaciones bases contiguas no usarán las mismas frecuencias para los radiocanales, por lo que se evitan más interferencias.

3.3.2 TDMA

En la técnica de acceso múltiple TDMA se asigna la misma frecuencia a los usuarios durante breves intervalos de tiempo periódicamente, de forma que todos transmiten a la vez pero de forma discontinua en el tiempo.

[13] Definición de canal físico y acceso múltiple según José María Hernando Rábanos en su libro Comunicaciones Móviles, 2ª edición.

El sistema se encarga de direccionar y sincronizar cada ráfaga de información que ha enviado el usuario a su destino, de manera que cada receptor sólo recibe las que le pertenecen ignorando las demás.

Por tanto, cada trama en TDMA se dividirá en intervalos de tiempo. Cada intervalo se asignará a una línea y esta podrá hacer uso de todo el ancho de banda del sistema.

3.3.4 CDMA

A diferencia de los anteriores, CDMA establece para cada canal todo el ancho de banda y todo el tiempo disponible, de tal forma que todos los usuarios están emitiendo en la misma frecuencia y a la vez.

Esta situación produce una intensa interferencia mutua, por lo que debe lograrse extraer la información de cada canal del conjunto de señales. Para ello, se asigna a cada comunicación un código único denominado código de dirección o signatura.

Cada comunicación tendrá su código combinado con la información transmitida, permitiendo así que tanto emisor como receptor puedan distinguir su comunicación de las diferentes señales transmitidas.

3.4 Sistema celular

El sistema celular consiste en dividir las zonas de cobertura en zonas más pequeñas denominadas celdas o células para poder reutilizar las frecuencias disponibles. Cada conjunto de frecuencias disponibles se repartirá entre un conjunto de células que formarán una agrupación o cluster, de forma que dentro de un cluster no se reutilizará ninguna frecuencia. Denominaremos la distancia cocanal o distancia de reutilización a la distancia entre dos células (de diferentes cluster) que utilizan las mismas frecuencias.

También se usarán antenas directivas en los vértices alternos de cada celda, formando así tres sectores por célula. Esto reduce el número de fuentes interferentes comparado con el uso de una antena omnidireccional en cada celda.

La sectorización supone ahorros de infraestructura ya que permite cubrir sectores de células vecinas y así reduce el número de estaciones base. Además tendremos una menor interferencia cocanal y por tanto una mayor capacidad en el sistema debido a una mayor reutilización de las frecuencias disponibles.

3.5 GSM (2G) y GPRS (2,5G)

GSM es el estándar de un sistema de telefonía móvil digital público y europeo, basado en los sistemas celulares, que surgió con el objetivo de sustituir a la telefonía analógica existente en ese momento, ya que esta no tenía suficiente capacidad para dar servicio a toda la demanda que se preveía.

Su implantación comenzó en 1992 y coincidió con la liberalización del servicio de telefonía móvil. Como consecuencia surgieron operadores nuevos, dando lugar a una competencia que fomentó el desarrollo de la telefonía móvil y redujo los precios del servicio para el público.

Las características de este sistema son las siguientes:

- Utiliza una modulación GMSK con $B_bT = 0{,}3$.
- La relación de protección cocanal es $\left(\frac{C}{I_c}\right) = 9\ dB$.
- Puede compensar hasta velocidades de 200 km/h (Dispersión Doppler).
- Puede ecualizarse como máximo una dispersión temporal de 16 μs.
- Se basa en una estructura celular sectorizada en ambientes urbanos y omnidireccional en zonas rurales.
- Acceso múltiple TDMA con 8 intervalos en cada trama (8 canales físicos): FDD/FDMA/TDMA.
- 200 KHz de separación entre canales.
- Los terminales móviles pueden cambiar hasta 217 veces por segundo de frecuencia de una trama a otra para evitar el desvanecimiento de la señal por multitrayecto (Frequency Hopping).
- Se transmite de forma discontinua en la conversación, ya que sólo se envía información mientras el usuario está hablando. Mientras el emisor no habla en el terminal receptor se genera un ruido de confort.
- Como medios de seguridad se utiliza el cifrado en las comunicaciones y la autenticación en el acceso al sistema.
- La localización automática se efectúa mediante la captación de la señal de control y el envío de su identidad a la red por parte del terminal.

La arquitectura de GSM se estructura en unidades funcionales e interfaces. Las unidades funcionales son las encargadas de la ejecución de las funciones del sistema, y las interfaces las fronteras que las separan.

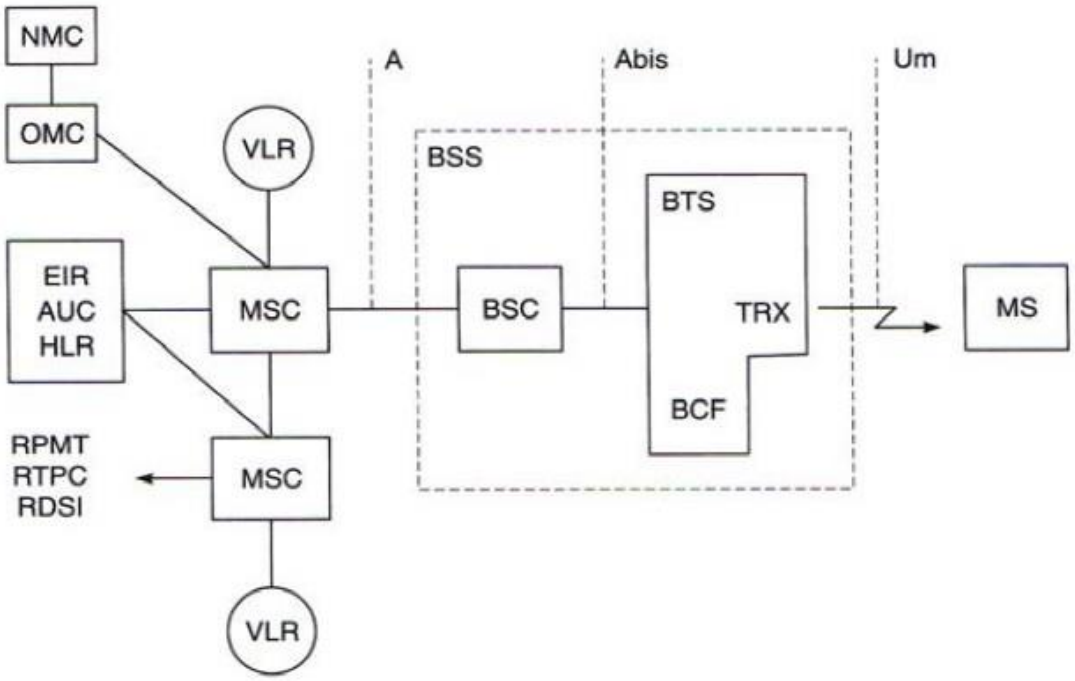


Ilustración 12/Arquitectura GSM[14]

Las unidades funcionales son las siguientes:

AUC: Centro de autentificación.
BCF: Funciones de control de la estación base.
BSC: Controlador de la estación base.
BSS: Sistema de estación base.
BTS: Transceptor de estación base.
EIR: Registro de identidad de equipos.
HLR: Registro de abonados.
MS: Estación móvil.
MSC: Centro de conmutación de servicios móviles.
NMC: Centro de gestión de red.
OMC: Centro de operación y mantenimiento.
RDSI: (ISDN) Red digital de servicios integrados.
RPMT: (PMLN) Red pública móvil terrestre.
RTPC: (PSTN) Red telefónica pública conmutada.
TRX: Transceptores.
VLR: Registro de visitantes.

[14] TEMA 4: REDES DE COMUNICACIONES MÓVILES TERRESTRES, GTT SISTEMAS DE TELECOMUNICACIÓN (2013/2014)

Existen dos interfaces básicas, la interfaz de línea "A" que separa el centro de conmutación y el sistema de estación base y la interfaz radio "Um" que delimita la frontera entre el sistema de estación base y el conjunto de estaciones móviles.

Para la identificación de una estación móvil serán necesarios dos identidades:

- IMEI: El código es grabado por el fabricante en el equipo e identifica el terminal.
- IMSI: Identifica al usuario a nivel internacional y está asociado a la tarjeta SIM.

En GSM cada trama está formada por 8 intervalos de tiempo, teniendo una duración cada uno de 0,577 ms y por tanto cada trama 4,615 ms.

La estructura de trama es idéntica para el enlace ascendente y para el descendente, solo que el ascendente tiene un desfase de 3 intervalos para que el terminal reciba y transmita en distintos instantes de tiempo.

La información de cada intervalo se transmite mediante ráfagas de 148 bits, a las que se le añaden 8,25 bits de guarda. Por tanto si cada intervalo dura 0,577 ms:

$$Velocidad\ de\ tx\ radio = \frac{156{,}25\ bits}{0{,}577\ ms} = 270{,}833\ kbps$$

Existen varios tipos de canales en GSM:

- Canales de tráfico: Los constituyen un par de portadoras e intervalos de tiempo asignados a un terminal para efectuar una comunicación. Estos canales son los denominados TCH.
- Canales de señalización asociados a cada llamada: Son los canales de señalización que se asocian a cada llamada de forma independiente. Existen dos tipos: SACCH (Slow Associated Control Channel) y FACCH (Fast Associated Control Channel).
- Canales de difusión: Son aquellos que sólo se transmiten de forma descendente y van dirigidos a todos los terminales, portando información general de orientación y sincronización. Los forman el BCCH (Broadcast Control Channel), el FCCH (Frequency Correction Channel) y el SCH (Synchronization Channel).
- Canales comunes: Se utilizan para regular el acceso de los terminales al sistema. Son el RACH (Random Access Channel), el PCH (Pagging Channel) y el AGCH (Access Grant Channel).
- Canales dedicados: Son canales bidireccionales que se asignan de forma exclusiva a los terminales durante la fase previa a la llamada. Los forman el SDCCH (Stand-alone Dedicated Control Channel) y el SACCH (Slow Associated Control Channel).

Debido a la necesidad de conseguir mayores velocidades para la transmisión de datos, el ETSI tomó la decisión a mediados de la década de los 90 de establecer un nuevo estándar. Este estándar conocido como GPRS estaría basado en la interfaz radio del sistema GSM, y permitiría una adecuada integración de los protocolos de Internet TCP/IP con la red móvil existente.

Por tanto se considera a GPRS como una transición entre los sistemas móviles de segunda generación (GSM) y los de tercera (UMTS).

Las características de este sistema en comparación con GSM son:

- Acceso radio en modo paquete y backbone IP.
- Incorpora dos nuevos nodos para conmutación de paquetes (SGSN y GGSN).
- Velocidad máxima teórica: 144 kbps.
- GPRS sólo utiliza los recursos de la red cuando hay datos que enviar o recibir.

El sistema GSM fue diseñado originalmente para un uso casi único de tráfico de voz. Por ello GPRS tiene como principal objetivo ofrecer un acceso a redes de datos como TCP/IP.

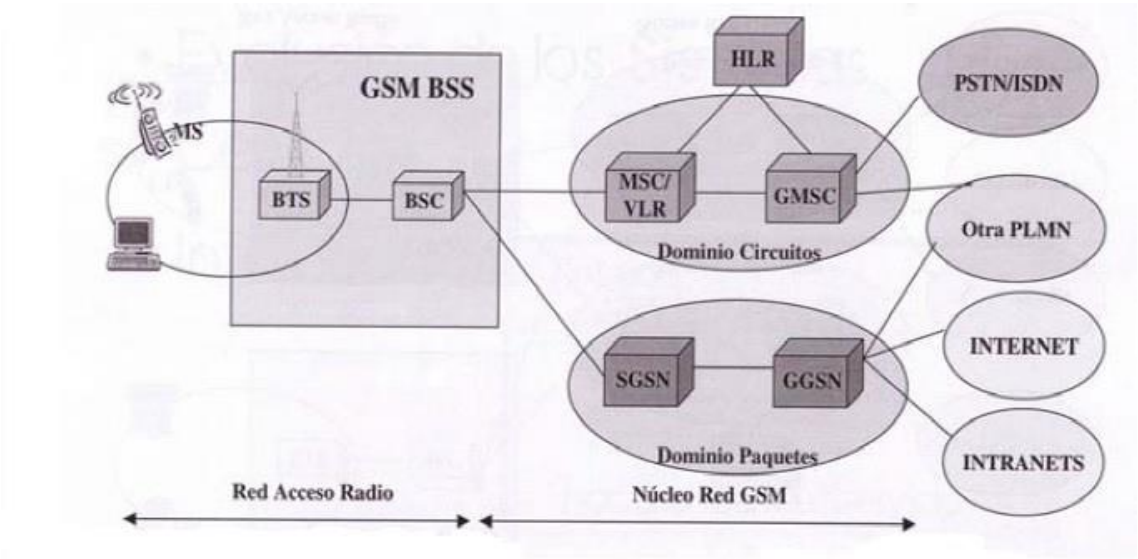


Ilustración 13/Arquitectura GPRS[15]

Como podemos comprobar en la arquitectura de GPRS, se reaprovecha la estructura del sistema GSM a la que se le añaden una serie de elementos:

- SGSN (Serving GPRS Suport Node): Servidor que soporta GPRS.
- GGSN (Gateway GPRS Suport Node): Ejerce de pasarela entre la red GPRS y redes públicas de datos como IP y X.25, conectando también con otras redes GPRS.
- GMSC (Gateway MSC).

[15] TEMA 4: REDES DE COMUNICACIONES MÓVILES TERRESTRES, GTT SISTEMAS DE TELECOMUNICACIÓN (2013/2014)

Como evoluciones de GPRS se presentan EDGE y EDGE Evolution. Ambos eran una extensión de GPRS con modulación/codificación adaptativa y requerían hardware nuevo en las estaciones base y en los terminales. Es por esto que EDGE, debido a no aumentar mucho sus prestaciones respecto a GPRS tuvo pocas previsiones de mercado. En cambio EDGE Evolution ofrecía hasta 1Mbps y así obtuvo una gran aceptación en el mercado.

3.6 UMTS (3G)

UMTS surge como una evolución de los sistemas GSM y GPRS con el objetivo de aumentar la velocidad (hasta 2 Mbps en entornos urbanos interiores) y estandarizar mundialmente el sistema de comunicación móvil.

Algunas de las novedades que incluirá este sistema son las siguientes: los servicios de voz obtendrán mayor capacidad, se utilizará la tecnología de paquetes desde el terminal hasta toda la red bajo el protocolo IP, los terminales serán reconfigurables y con capacidad de descarga de servicios y aplicaciones.

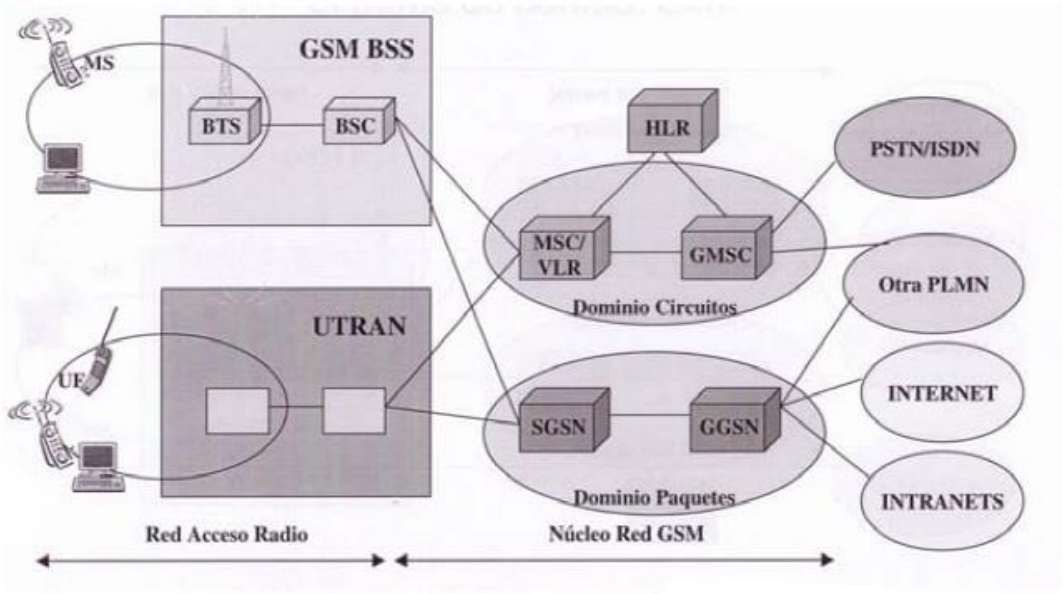


Ilustración 14/Arquitectura UMTS[16]

Si observamos la arquitectura de UMTS, podemos comprobar cómo se ha incluido un nuevo elemento: UTRAN, UMTS Terrestial Radio Access Network.

La red troncal de UMTS realiza labores de transporte de información, tanto del tráfico como de la señalización. También realiza el encaminamiento de las llamadas y la gestión de la movilidad, además de conectarse a otras redes.

[16] TEMA 4: REDES DE COMUNICACIONES MÓVILES TERRESTRES, GTT SISTEMAS DE TELECOMUNICACIÓN (2013/2014)

Al ser una evolución de la arquitectura GSM+GPRS, contiene los mismos elementos a excepción de la UTRAN. Los dominios de paquetes y circuitos se mantendrán separados y conectados entre sí, aunque la tendencia será una única red IP.

Las unidades funcionales de la UTRAN son las equivalentes a las del BSS en GSM:

- BTS -> GSM
- BSC -> RNC

Además se añade una nueva interfaz entre RNCs que no existía en GSM, la interfaz normalizada "Iur".

UMTS utiliza el sistema de acceso múltiple CDMA de banda ancha, WCDMA. Se trata de una técnica de espectro ensanchado en la que todos los usuarios de la celda comparten la misma portadora y distinguen su señal con el uso de distintos códigos. A diferencia de GSM donde la portadora ocupaba 200 KHz, en UMTS se necesitan 5 MHz por portadora.

Al igual que en GPRS, en UMTS también se consiguió mejorar la velocidad, tanto de bajada (HSDPA) como de subida (HSUPA) y reducir la latencia de los servicios de datos. Esto se consiguió gracias al uso de una modulación/codificación adaptativa, a la asignación rápida de recursos y a los mecanismos de transmisión híbridos (HARQ). También cambió la gestión de los recursos radio, ya que en lugar de mantener una tasa binaria constante variando la potencia de transmisión, se intenta utilizar la máxima tasa binaria con la potencia disponible.

Con HSPA+, que hace uso de 2 portadoras simultáneas de 5 MHz, se obtienen velocidades de hasta 23 Mbps en subida y 84 Mbps en bajada.

3.7 LTE

La necesidad de un nuevo sistema de telefonía móvil era clara:

- Había que asegurar la continuidad de la competitividad de los sistemas 3G en el futuro.
- El usuario demandaba mayores tasas y calidad de servicios.

El objetivo era lograr un sistema optimizado para paquetes, de baja complejidad y reduciendo costes de capital y de operación.

En la siguiente tabla podemos ver cómo han avanzado los sistemas móviles desde GSM hasta LTE.

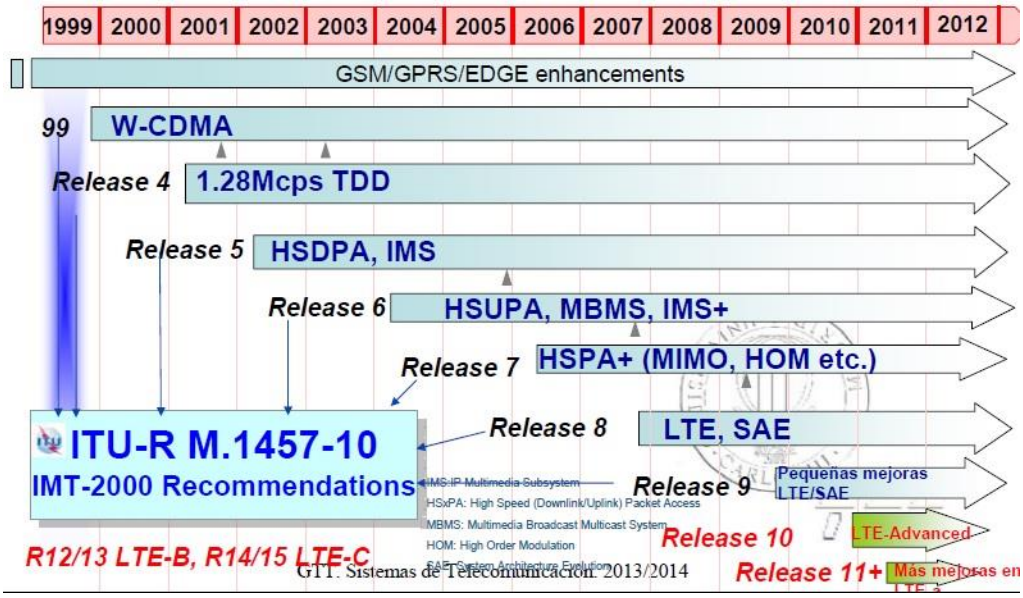


Ilustración 15/Releases[17]

Estos cambios también han tenido lugar en la arquitectura, ya que LTE está orientado fundamentalmente a transporte de paquetes. Así pues, el NodeB de UMTS pasará a ser eNodeB en LTE y se encargará de la gestión de recursos radio, sincronización y control de interferencias, compresión de cabeceras IP, cifrado y protección de la integridad de datos de usuario, la selección del MME (Mobile Management Entity) y el encaminamiento en ambos sentidos hasta el S-GW (Serving Gateway). Entre los eNodeB aparecerá una nueva interfaz, la X2, que realizará los traspasos, balances de carga y cancelación de interferencias. A este conjunto se le denominará EUTRAN (Envolved UTRAN). Se usará otra nueva interfaz para la comunicación entre los eNodeB y los MME/S-GW.

[17] TEMA 4: REDES DE COMUNICACIONES MÓVILES TERRESTRES, GTT SISTEMAS DE TELECOMUNICACIÓN (2013/2014)

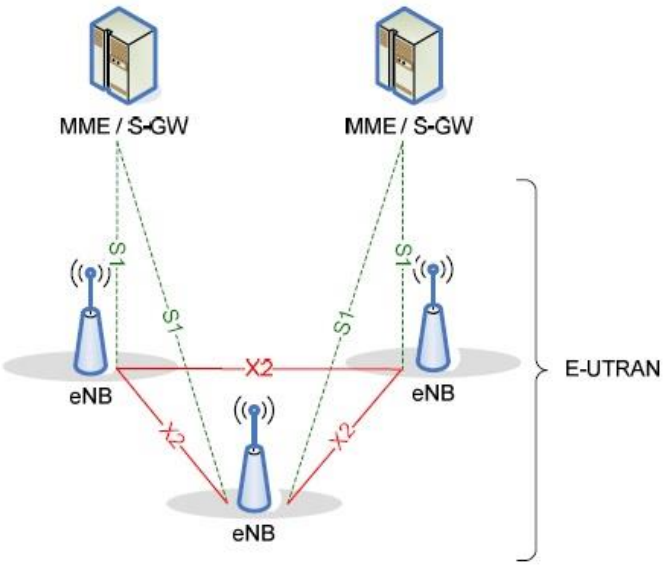


Ilustración 16/Arquitectura LTE[18]

Con LTE se alcanzarán velocidades teóricas de hasta 326.4Mbps en bajada y 86.4 Mbps en subida.

[18] ETSI TS 136 300 V9.10.0 (2013-02), FIGURE 4-1: OVERALL ARCHITECTURE

4. Aspectos teóricos de LTE

Para poder implementar nuestro inhibidor de LTE, es fundamental conocer ciertos aspectos teóricos que serán fundamentales en el desarrollo de la aplicación.

Ya hemos comentado los métodos de acceso múltiple más básicos: FDMA, TDMA y CDMA. En el caso de LTE se usará OFDMA para el enlace descendente, un método de acceso múltiple basado en FDMA con las portadoras ortogonales (subportadoras), de forma que se pueden utilizar más portadoras con un menor ancho de banda y unidas bajo una sola frecuencia (portadora).

Así pues, todos los usuarios estarán conectados a la misma frecuencia (usan la misma portadora), pero a cada usuario le corresponderán una o varias subportadoras, de forma que con una sola frecuencia de portadora y un ancho de banda de hasta 20 MHz podemos dar servicio a múltiples usuarios.

En LTE se combina OFDMA con TDMA, de forma que cada subportadora será usada por un usuario en un determinado instante de tiempo. En la siguiente ilustración se muestra claramente el concepto de división en tiempo y frecuencia simultáneamente.

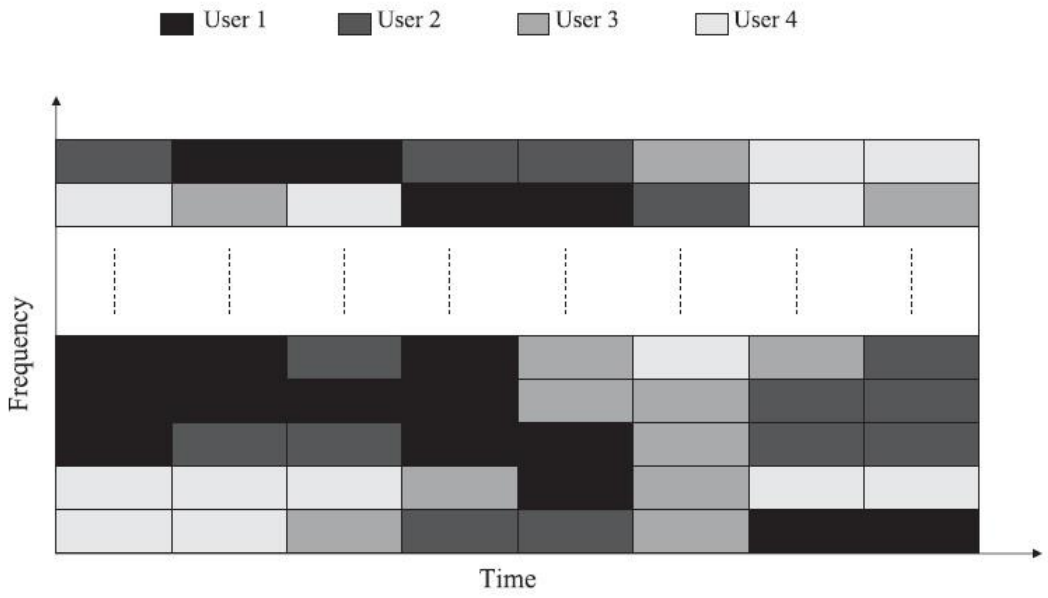


Ilustración 17/División por Frecuencia y Tiempo[19]

[19] LTE – THE UMTS LONG TERM EVOLUTION, SECOND EDITION. STEFANIA SESIA, ISSAM TOUFIK, MATTHEW BAKER. FIGURE 5.12

La forma de la trama en LTE es diferente si usamos FDD (Frequency Division Duplexing) que si usamos TDD (Time Division Duplexing). Nos centraremos en el primer caso, ya que actualmente es el método usado en España. FDD consiste en utilizar distinta frecuencia para la subida y para la bajada. En la siguiente ilustración podemos ver un ejemplo de trama LTE usando FDD.

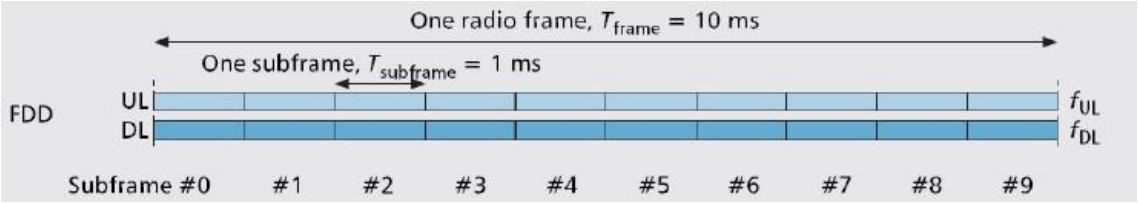


Ilustración 18/FDD[20]

Cada trama tiene una duración de 10 ms. Esta se divide en 10 subtramas de 1 ms, que se subdividen a su vez en 2 slot cada una de 0,5 ms de duración, quedando una estructura de trama como la siguiente:

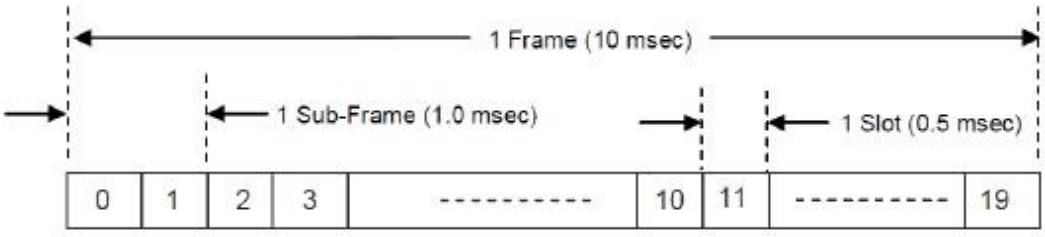


Ilustración 19/Estructura de trama[21]

El número de símbolos OFDMA que se transmitirán en cada slot dependerá del prefijo cíclico que usemos:

- Prefijo cíclico normal: 7 símbolos OFDMA.
- Prefijo cíclico extendido: 6 símbolos OFDMA.

El prefijo cíclico consiste en insertar al inicio de cada símbolo OFDMA las últimas subportadoras de este como sustitutivo del espacio de guarda entre símbolos. De no usarlo y dejar un espacio vacío de guarda se perdería ortogonalidad entre símbolos, lo que no favorecería a una buena transmisión.

En nuestro caso usaremos el prefijo cíclico normal, ya que su uso es más común en ciudad, a diferencia del prefijo cíclico extendido que se suele utilizar en zonas rurales.

[20] TEMA 4: REDES DE COMUNICACIONES MÓVILES TERRESTRES, GTT SISTEMAS DE TELECOMUNICACIÓN (2013/2014)

[21] http://www.sharetechnote.com/html/FrameStructure_DL.html#Overview

De esta manera la estructura de cada slot quedaría como sigue:

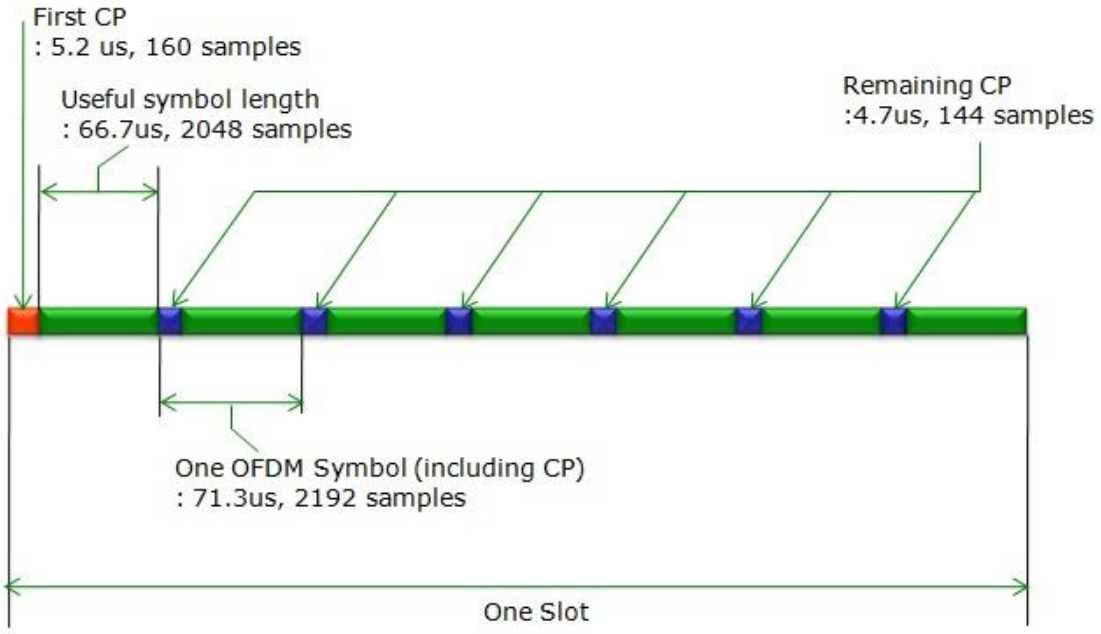


Ilustración 20/Estructura de un slot para un ancho de banda de 20 MHz[22]

Como se puede comprobar, el primer prefijo cíclico dura más muestras que los otros seis. Los valores de tiempo y muestras de este ejemplo serían los adecuados para la transmisión usando un ancho de banda por símbolo de 20 MHz, pero como hemos comentado anteriormente, en LTE se puede transmitir con diferentes anchos de banda. Veamos las características estructurales dependiendo del ancho de banda.

BW	1.4 MHz	2.5 MHz	5 MHz	10 MHz	15 MHz	20 MHz
Espacio entre subportadoras	15 KHz					
Frecuencia de muestreo	1.92 MHz	3.84 MHz	7.68 MHz	15.36 MHz	23.04 MHz	30.72 MHz
Tamaño FFT	128	256	512	1024	1536	2048
Resource Blocks	6	15	25	50	75	100
Longitud de prefijo cíclico (muestras)	1º-> 10 resto-> 9	1º-> 20 resto-> 18	1º-> 40 resto-> 36	1º-> 80 resto-> 72	1º-> 120 resto-> 108	1º-> 160 resto-> 144

Tabla 5/Parámetros OFDMA en función del BW

[22] http://www.sharetechnote.com/html/FrameStructure_DL.html#Overview

En la tabla anterior aparece un elemento que aún no hemos comentado, el Resource Block. Este elemento ocupa en tiempo un slot (7 símbolos OFDMA) y en frecuencia 12 Resource Elements. Un Resource Element es una subportadora en frecuencia y un símbolo OFDMA en tiempo. En la siguiente ilustración se muestra una trama para 1,4 MHz de ancho de banda con los Resource Blocks y los Resource Elements.

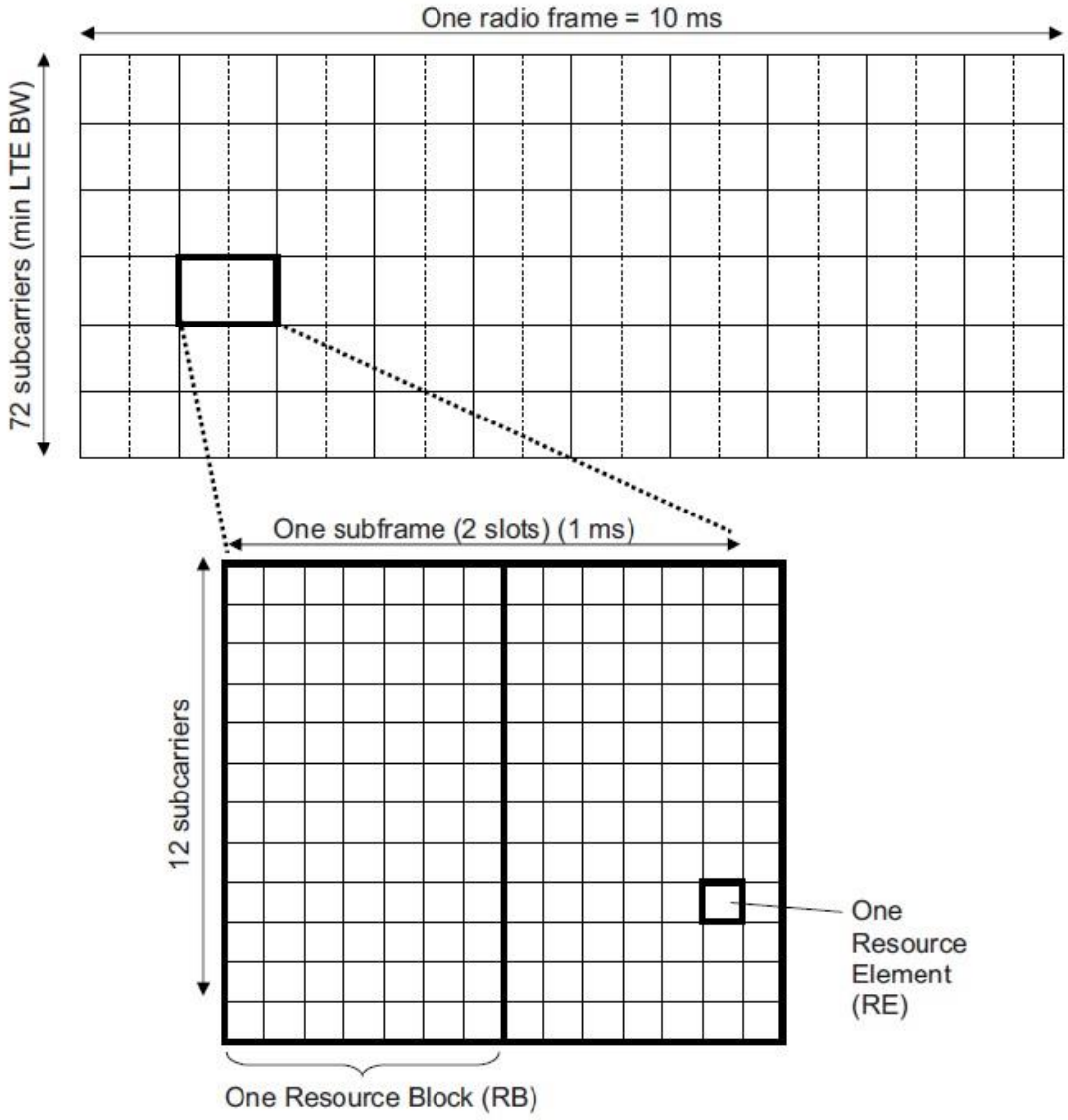


Ilustración 21/Resource Blocks y Resource Elements[23]

[23] LTE – THE UMTS LONG TERM EVOLUTION, SECOND EDITION. STEFANIA SESIA, ISSAM TOUFIK, MATTHEW BAKER. FIGURE 6.1

En el enlace descendente encontraremos los siguientes elementos:

- Canales físicos: transportan información de niveles superiores como el de transporte.
- Señales físicas: no transportan información, sirven de apoyo al nivel físico.

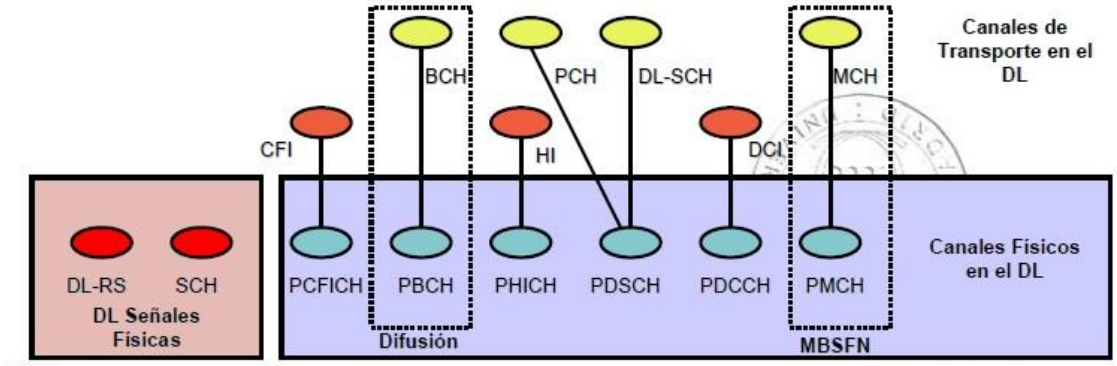


Ilustración 22/Canales y señales DL LTE[24]

Tanto los canales físicos como las señales físicas viajarán en la trama (FDD) repartidos en grupos de Resource Elements de la siguiente forma:

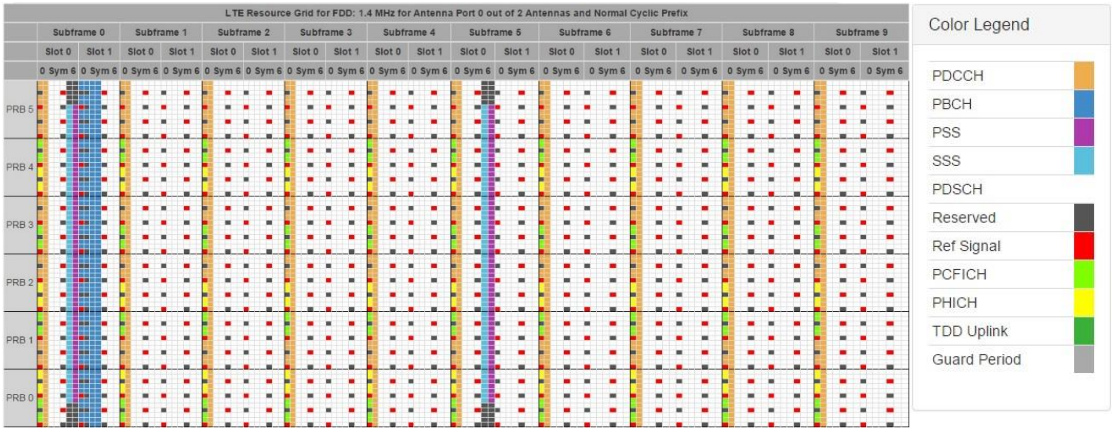


Ilustración 23/Trama con canales y señales físicas[25]

El SCH es el canal de sincronización, y está compuesto de dos señales físicas: la PSS, Primary Sinchronization Signal y la SSS, Secondary Sinchronization Signal. Estas señales sirven para que el terminal establezca conexión con el eNodeB.

Las señales de sincronización dependen de dos constantes definidas por el ID de la célula como sigue:

$$N_{ID}^{cell} = 3N_{ID}^{1} + N_{ID}^{2}$$

Donde $0 \leq N_{ID}^{1} \leq 167$ y $0 \leq N_{ID}^{2} \leq 2$.

[24] TEMA 4: REDES DE COMUNICACIONES MÓVILES TERRESTRES, GTT SISTEMAS DE TELECOMUNICACIÓN (2013/2014)
[25] http://dhagle.in/LTE

La PSS sincroniza el terminal en tiempo y en frecuencia y proporciona el N_{ID}^2. Se genera a partir de una secuencia Zadoff-Chu en el dominio de la frecuencia tal y como sigue:

$$d_u(n) = \begin{cases} e^{-j\frac{\pi un(n+1)}{63}} & n = 0,1,\ldots,30 \\ e^{-j\frac{\pi u(n+1)(n+2)}{63}} & n = 31,32,\ldots,61 \end{cases}$$

Donde el índice *u* se obtiene a partir de la siguiente tabla:

$N_{\mathrm{ID}}^{(2)}$	Root index *u*
0	25
1	29
2	34

Ilustración 24/NID2 y U[26]

Para el tipo de trama que usaremos (FDD y prefijo cíclico normal), los 62 valores de la PSS se transmitirán del 5º al 66º Resource Element, ambos inclusive, del 7º símbolo OFDMA de los slot 0 y 10, quedando los 5 primeros y últimos Resource Elements del símbolo inutilizados.

De la SSS se obtiene el tipo de duplexación (FDD/TDD), el tipo de prefijo cíclico (Normal/Extendido) y el N_{ID}^1. La SSS se divide en dos señales, una que se transportará en la primera subtrama y otra en la sexta. Cada una se genera mediante la concatenación de dos secuencias de tamaño 31 como sigue:

$$d(2n) = \begin{cases} s_0^{(m_0)}(n)c_0(n) & \text{in subframe 0} \\ s_1^{(m_1)}(n)c_0(n) & \text{in subframe 5} \end{cases}$$

$$d(2n+1) = \begin{cases} s_1^{(m_1)}(n)c_1(n)z_1^{(m_0)}(n) & \text{in subframe 0} \\ s_0^{(m_0)}(n)c_1(n)z_1^{(m_1)}(n) & \text{in subframe 5} \end{cases}$$

Donde $0 \leq n \leq 30$.

Las secuencias $s_0^{m_0}(n)$ y $s_1^{m_1}(n)$ se consiguen de forma que:

$$s_0^{(m_0)}(n) = \tilde{s}((n+m_0) \bmod 31)$$
$$s_1^{(m_1)}(n) = \tilde{s}((n+m_1) \bmod 31)$$

[26] ETSI TS 136 300 V9.10.0 (2013-02), TABLE 6.11.1.1-1

Donde:

$$\tilde{s}(i) = 1 - 2x(i),\ 0 \le i \le 30$$

Es definida por:

$$x(\bar{i}+5) = \left(x(\bar{i}+2) + x(\bar{i})\right) \bmod 2, \qquad 0 \le \bar{i} \le 25$$

Con condiciones iniciales:

$$x(0) = 0, \quad x(1) = 0, \quad x(2) = 0, \quad x(3) = 0, \quad x(4) = 1$$

Las secuencias $c_0(n)$ y $c_1(n)$ se consiguen de forma que:

$$c_0(n) = \tilde{c}((n + N_{\mathrm{ID}}^{(2)}) \bmod 31)$$
$$c_1(n) = \tilde{c}((n + N_{\mathrm{ID}}^{(2)} + 3) \bmod 31)$$

Donde:

$$\tilde{c}(i) = 1 - 2x(i),\ 0 \le i \le 30$$

Es definida por:

$$x(\bar{i}+5) = \left(x(\bar{i}+3) + x(\bar{i})\right) \bmod 2, \qquad 0 \le \bar{i} \le 25$$

Con condiciones iniciales:

$$x(0) = 0, \quad x(1) = 0, \quad x(2) = 0, \quad x(3) = 0, \quad x(4) = 1$$

Las secuencias $z_1^{m_0}(n)$ y $z_1^{m_1}(n)$ se consiguen de forma que:

$$z_1^{(m_0)}(n) = \tilde{z}((n + (m_0 \bmod 8)) \bmod 31)$$

$$z_1^{(m_1)}(n) = \tilde{z}((n + (m_1 \bmod 8)) \bmod 31)$$

Donde:

$$\tilde{z}(i) = 1 - 2x(i),\ 0 \le i \le 30$$

Es definida por:

$$x(\bar{i}+5) = \left(x(\bar{i}+4) + x(\bar{i}+2) + x(\bar{i}+1) + x(\bar{i})\right) \bmod 2, \qquad 0 \le \bar{i} \le 25$$

Con condiciones iniciales:

$$x(0) = 0, \quad x(1) = 0, \quad x(2) = 0, \quad x(3) = 0, \quad x(4) = 1$$

Los índices m_0 y $m_1$se obtienen a partir del N_{ID}^1 y vienen definidos en la siguiente tabla.

$N_{ID}^{(1)}$	m_0	m_1	$N_{ID}^{(1)}$	m_0	m_1	$N_{ID}^{(1)}$	m_0	m_1	$N_{ID}^{(1)}$	m_0	m_1	$N_{ID}^{(1)}$	m_0	m_1
0	0	1	34	4	6	68	9	12	102	15	19	136	22	27
1	1	2	35	5	7	69	10	13	103	16	20	137	23	28
2	2	3	36	6	8	70	11	14	104	17	21	138	24	29
3	3	4	37	7	9	71	12	15	105	18	22	139	25	30
4	4	5	38	8	10	72	13	16	106	19	23	140	0	6
5	5	6	39	9	11	73	14	17	107	20	24	141	1	7
6	6	7	40	10	12	74	15	18	108	21	25	142	2	8
7	7	8	41	11	13	75	16	19	109	22	26	143	3	9
8	8	9	42	12	14	76	17	20	110	23	27	144	4	10
9	9	10	43	13	15	77	18	21	111	24	28	145	5	11
10	10	11	44	14	16	78	19	22	112	25	29	146	6	12
11	11	12	45	15	17	79	20	23	113	26	30	147	7	13
12	12	13	46	16	18	80	21	24	114	0	5	148	8	14
13	13	14	47	17	19	81	22	25	115	1	6	149	9	15
14	14	15	48	18	20	82	23	26	116	2	7	150	10	16
15	15	16	49	19	21	83	24	27	117	3	8	151	11	17
16	16	17	50	20	22	84	25	28	118	4	9	152	12	18
17	17	18	51	21	23	85	26	29	119	5	10	153	13	19
18	18	19	52	22	24	86	27	30	120	6	11	154	14	20
19	19	20	53	23	25	87	0	4	121	7	12	155	15	21
20	20	21	54	24	26	88	1	5	122	8	13	156	16	22
21	21	22	55	25	27	89	2	6	123	9	14	157	17	23
22	22	23	56	26	28	90	3	7	124	10	15	158	18	24
23	23	24	57	27	29	91	4	8	125	11	16	159	19	25
24	24	25	58	28	30	92	5	9	126	12	17	160	20	26
25	25	26	59	0	3	93	6	10	127	13	18	161	21	27
26	26	27	60	1	4	94	7	11	128	14	19	162	22	28
27	27	28	61	2	5	95	8	12	129	15	20	163	23	29
28	28	29	62	3	6	96	9	13	130	16	21	164	24	30
29	29	30	63	4	7	97	10	14	131	17	22	165	0	7
30	0	2	64	5	8	98	11	15	132	18	23	166	1	8
31	1	3	65	6	9	99	12	16	133	19	24	167	2	9
32	2	4	66	7	10	100	13	17	134	20	25	-	-	-
33	3	5	67	8	11	101	14	18	135	21	26	-	-	-

Ilustración 25/NID1, M0 y M1[27]

Para el tipo de trama que usaremos (FDD y prefijo cíclico normal), los 62 valores de la SSS que viaja en la subtrama 0 se transmitirán del 5º al 66º Resource Element, ambos inclusive, del 6º símbolo OFDMA del slot 0, quedando los 5 primeros y últimos Resource Elements del símbolo inutilizados. Los 62 valores de la SSS que viaja en la subtrama 5 se transmitirán del 5º al 66º Resource Element, ambos inclusive, del 6º símbolo OFDMA del slot 10, quedando los 5 primeros y últimos Resource Elements del símbolo inutilizados.

[27] ETSI TS 136 300 V9.10.0 (2013-02), TABLE 6.11.2.1-1

5. Descripción de la aplicación

5.1 Descripción teórica

Como ya hemos comentado, nuestra aplicación consiste en realizar un inhibidor de frecuencia para LTE haciendo uso de la herramienta de trabajo LabVIEW y del hardware NI USRP 2920. Para ello nos basaremos en la patente "WO2014041225 A1" de la UC3M, que explica cómo se pueden conseguir muy buenos resultados "atacando" al canal de sincronización (SCH) en el enlace de bajada.

La invención de la patente consiste en transmitir el SCH desplazado en tiempo (el inhibidor no está sincronizado en tiempo con el eNodeB), consiguiendo así interferir a la señal original del eNodeB e impidiendo que el terminal sea incapaz de conectarse a la red. Nuestra aplicación será por tanto desarrollar un transmisor LTE con unas determinadas características.

Dado que lo único que precisamos transmitir es el SCH, será suficiente el uso de un ancho de banda de 1.4 MHz. La razón es que los canales y las señales físicas se transportan en la banda central de la portadora LTE (1.4 MHz). A excepción del SCH, lo que se transmitirá en ese ancho de banda serán "ceros" (todos los bits de la cadena de bits de entrada son 0) modulados con una QPSK. En el caso del SCH serán la PSS y la SSS las señales que se transmitirán. Que sólo se transmita el SCH nos permitirá ahorrarnos complejidad y potencia de transmisión.

Dadas estas características la trama LTE no va a sufrir variaciones respecto al tiempo, por lo que definiremos todos sus valores en un array y la transmitiremos continuamente haciendo uso de un bucle.

Podemos acordar, por tanto, que tendremos cuatro símbolos OFDMA diferentes, uno con "ceros" modulados, otro con la PSS y dos con la SSS (son dos señales). Ordenados según la estructura de la trama obtendremos la trama completa.

La señal de bits modulada se consigue pasando cada grupo de 2 bits por un modulador QPSK, resultando un número complejo de entre los 4 posibles (siendo $x = I + jQ$):

$b(i), b(i+1)$	I	Q
00	$1/\sqrt{2}$	$1/\sqrt{2}$
01	$1/\sqrt{2}$	$-1/\sqrt{2}$
10	$-1/\sqrt{2}$	$1/\sqrt{2}$
11	$-1/\sqrt{2}$	$-1/\sqrt{2}$

Ilustración 26/QPSK

Cada número complejo será un resource element, y serán necesarios 72 para formar el símbolo OFDMA. Para completar el tamaño 128 de la IFFT, rellenaremos el array con ceros arriba y abajo a partes iguales, de forma que tendremos 28 por arriba y 28 por abajo.

Las señales de sincronización se obtendrán como se explica en el capítulo 4. Tienen un tamaño de 62 resource elements, por lo que actuaremos igual que con la secuencia de bits: rellenaremos el array con ceros arriba y abajo a partes iguales hasta completar el tamaño 128 de la IFFT (33 ceros por arriba y 33 ceros por abajo).´l

Una vez tenemos las 4 señales en el dominio de la frecuencia de tamaño 128, se hará la IFFT a cada una, obteniendo así otro array de tamaño 128 para cada señal pero en el dominio del tiempo, y con cada símbolo ortogonal entre sí.

Para realizar la IFFT es necesario intercambiar los segundos 64 símbolos por los primeros, es decir, los símbolos del 64 al 127 ocuparán las posiciones desde la 0 hasta la 63, y los símbolos del 0 al 63 ocuparán las posiciones desde la 64 hasta la 127. De esta manera, el símbolo OFDMA tendrá los 72 resource elements (los 72 símbolos modulados) centrados en la frecuencia de portadora, dejando a cada lado los ceros de relleno insertados para realizar la IFFT de tamaño 128.

Nuestro símbolo OFDMA ocupará 1,08 MHz de ancho de banda:

$$15\ \frac{KHz}{Resource\ Element}\ x\ 72\ Resource\ Elements = 1{,}08\ MHz$$

Dejando 160 KHz de banda de guarda a cada lado del símbolo OFDMA, obtenemos los 1,4 MHz que necesitamos para transmitir la banda de canales y señales físicas de LTE:

Transmitiremos la PSS en el séptimo símbolo del primer slot y del undécimo. La primera SSS se transmitirá en el sexto símbolo del primer slot y la segunda en el sexto símbolo del undécimo slot. En el resto de los símbolos OFDMA transmitiremos los “ceros” modulados.

El diagrama de este proceso es el siguiente:

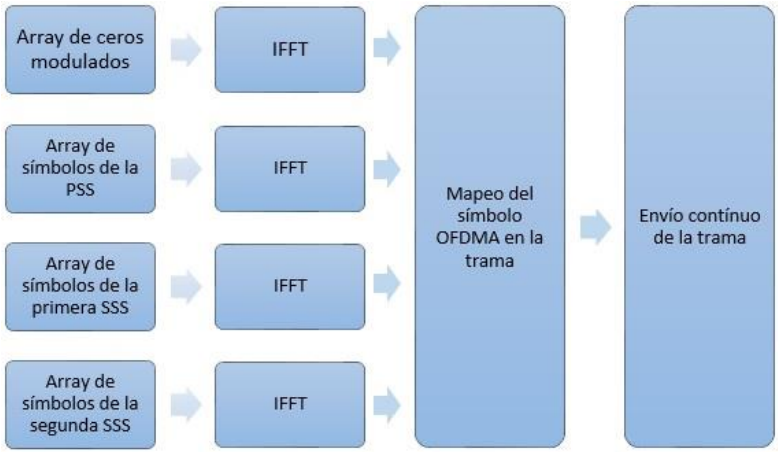


Ilustración 27/Diagrama de flujo

En la siguiente imagen podemos ver los 1,4 MHz de nuestro símbolo OFDMA recibido por el espectrómetro del laboratorio:

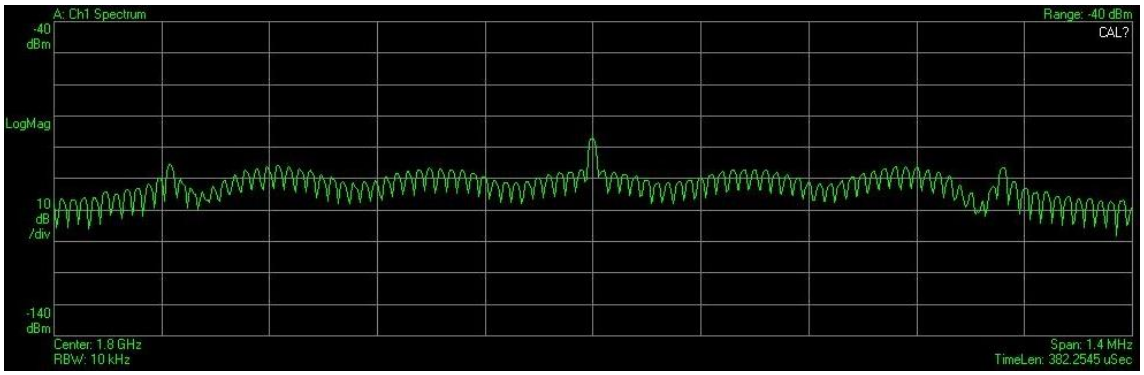


Ilustración 28/Símbolo OFDMA

5.2 Descripción gráfica

La interfaz gráfica de nuestra aplicación será la siguiente:

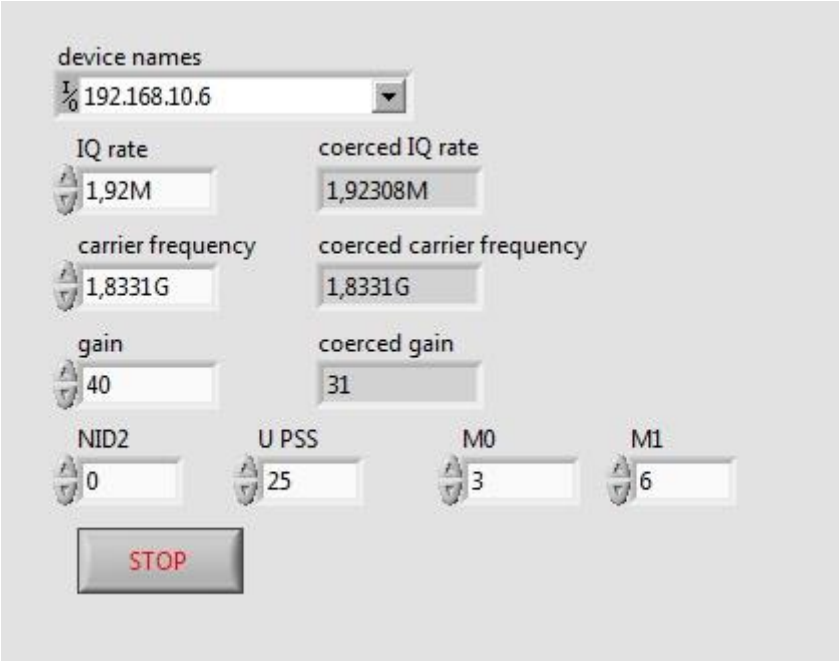


Ilustración 29/Interfaz gráfica de la aplicación[28]

Cada elemento se describe a continuación:

- Device names: se introduce la dirección IP del NI USRP 2920, que se conecta a través de un cable gigabit Ethernet a nuestro ordenador.
- IQ rate: se introduce la frecuencia de muestreo. En nuestro caso será de 1,92 MHz. La variable coerced IQ rate representa el valor real que se está usando durante la ejecución de la aplicación.

[28] Captura de pantalla de nuestra aplicación sobre LabVIEW.

- Carrier frequency: se introduce la frecuencia de portadora. En ella irá centrada nuestra señal. Su valor[29] dependerá de la operadora que queramos inhibir: Movistar (1817,1 MHz), Vodafone (1833,1 MHz), Yoigo (1854,1 MHz) y Orange (1874,9 MHz). Las operadoras virtuales harán roaming sobre una de estas cuatro operadoras. La variable coerced carrier frequency representa el valor real que se está usando durante la ejecución de la aplicación.
- Gain: se introduce la ganancia que se desea usar en el NI USRP 2920. Su valor máximo es 31, y es el que utilizaremos. La variable coerced gain representa el valor real que se está usando durante la ejecución de la aplicación.
- NID2: se introduce la constante N_{ID}^{2} ya que es necesaria para el cálculo de la SSS.
- U PSS: se introduce el valor de la constante U para el cálculo de la PSS. Este valor se obtiene del N_{ID}^{2} como se muestra en la "Ilustración 19/NID2 y U".
- M0 y M1: se introducen los valores de las constantes M0 y M1 para el cálculo de la SSS. Estos valores se obtienen del N_{ID}^{1} como se muestra en la "Ilustración 20/NID1, M0 y M1".
- STOP: se utiliza para detener la aplicación.

El valor N_{ID}^{cell} necesario para la elección de los valores NID2, U PSS, M0 y M1 será escogido al azar de entre los posibles valores: $0 \leq N_{ID}^{cell} \leq 503$

[29] Estos valores han sido obtenidos realizando una búsqueda exhaustiva sobre el espectrómetro. Los resultados inducen a que sólo se transmite LTE en la banda DCS. Esto es así en el campus de la UC3M de Leganés, pero en otras ciudades como Madrid se pueden encontrar portadoras de LTE en otras bandas. En este caso habría que utilizar más NI USRP 2920, uno para cada frecuencia que posea una operadora.

6. Conclusions

6.1 Tests and results

As it has been mentioned throughout this report, the goal of this application is clear: leave without LTE service the terminals connected to a specific operator. To inhibit more than an operator at the same time, it will be necessary to connect as much NI USRP 2920 as operators we want to inhibit. In any case, tests we will carry out are based in the inhibition of just one operator.

It were carried out tests for different operators and several user equipment, ending all of them successfully.

It has an inhibition radius between 15 cm and 1,5 m, depending on the operator, because each carrier arrives with different power. To increase this radius, it was tried to combine two SSS at random, so that the signal correlation increases and it can be more effective because the original SSS of the eNodeB is not known.

Results are not positive; using the same terminal and the same operator we obtained 22 cm of inhibition radius with an SSS at random and with the combination of two SSS at random we got a radius of 8 cm.

Everything seemed a success until it was tried with a Samsung Galaxy Note LTE terminal 4, which was able to keep the connection under the inhibition radius. This is because the terminal does not use the synchronization signals to keep the connection; it stores them in its memory. This user equipment only use the synchronization signals to establish the connection. Therefore we will try to connect the user equipment to LTE, it being under the inhibition radius, being that to establish the connection is strictly necessary to use the synchronization signals.

Indeed, the terminal is unable to connect to LTE under the inhibition radius, but is able to keep the connection if it was already established previously.

Therefore it can be affirmed that our application inhibits all cases, even though not always with the same effectivity because many factors are involved.

6.2 Efficiency

To check the effectiveness of our inhibitor is necessary to measure the power[30] transmitted over the inhibition radius to different lengths of the radius and compare it with the theoretical power transmitted at each point according to the basic propagation losses equation:

$$L_{bf}(dB) = 32{,}45 + 20\log f(MHz) + 20\log d(km)$$

[30] All power measurements are made for a bandwidth of 1.4 MHz. For the inhibitor's transmission power measurements 1800 MHz was used as frequency carrier.

Using this formula can be calculated the theoretical transmitted power, taking as reference the transmission power measured in the edge of the antenna, -34 dBm. In this graphic can be seen the comparison between theoretical and measured power:

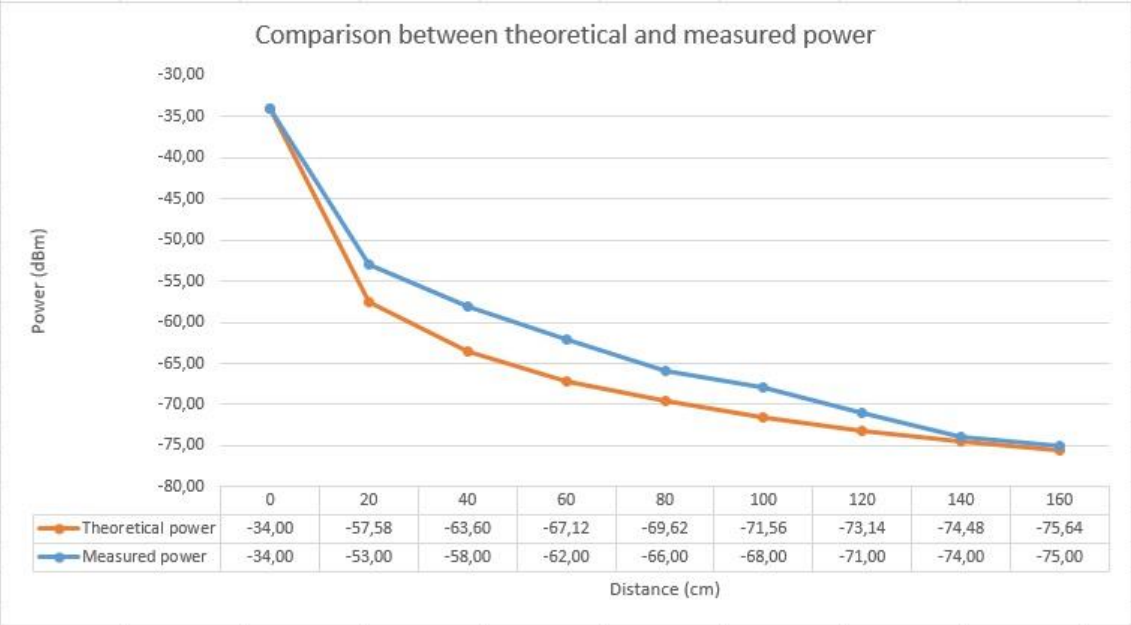


Figure 30/Comparison between theoretical and measured power

As shown, the measured power is quite similar to the theoretical, which shows that our results are right. Sometimes it there is a power difference of even 5dB, which can be because of the interferences produced in the place where measures have been taken.

Power received by each operator is as follows:

Operator	Power
Movistar	-83 dBm
Vodafone	-61 dBm
Yoigo	-72 dBm
Orange	-54 dBm

Table 6/Operator's power

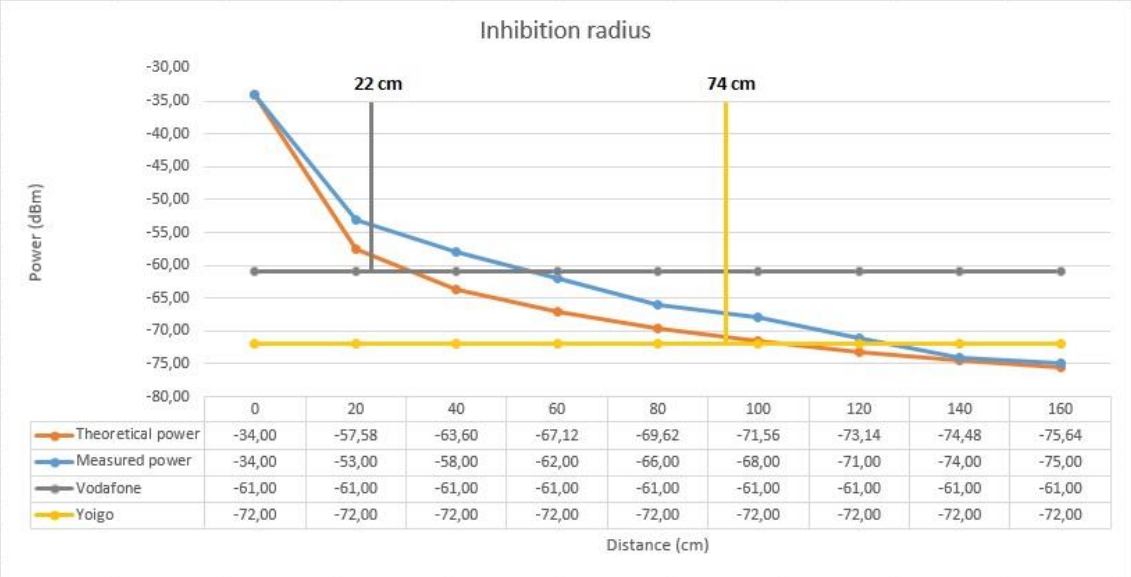
In the case of Vodafone, it has an inhibition radius of 22cm. The power that we measured in that point is approximately[31] -53dBm, and the Vodafone one is -61 dBm. Therefore, it can be said that to inhibit is necessary to interfere in the original signal in more than 8dB.

[31] We use the power measured at a distance of 20 cm because it is the closest to 22 cm.

However, if the same appreciation is done to the theoretical power[32] value in that point, -58,40dB, that is more accurate because it is not taken into account interferences, it can be determined that to inhibit is only necessary to interfere in the original signal in more than 2,6 dB.

A similar case is Yoigo. Here we have a 74 cm inhibition radius. The measured power at this point (80 cm) is -66 dBm and the Yoigo signal has a power of -72 dBm. Because of this we need to interfere the original signal with over 6 dB. If we do compare with the theoretical value, -68,94 dBm, we need to interfere the original signal with over 3 dB.

In the following figure we can see this values in opposition to the theoretical and measured power values:



	0	20	40	60	80	100	120	140	160
Theoretical power	-34,00	-57,58	-63,60	-67,12	-69,62	-71,56	-73,14	-74,48	-75,64
Measured power	-34,00	-53,00	-58,00	-62,00	-66,00	-68,00	-71,00	-74,00	-75,00
Vodafone	-61,00	-61,00	-61,00	-61,00	-61,00	-61,00	-61,00	-61,00	-61,00
Yoigo	-72,00	-72,00	-72,00	-72,00	-72,00	-72,00	-72,00	-72,00	-72,00

Figure 31/Inhibition radius

This is a very positive result with regard to the efficiency of our device, being that currently inhibitors need to interfere the original signal in more than 30 dB.

6.3 Budget

The material necessary to carry out this Bachelor Thesis are detailed below:

- LabVIEW Student Edition licence, necessary for the implementation of the application. It is a free version because is used for the realization of a Bachelor Thesis.
- NI USRP 2920, necessary for the realization of the application. Its price is about 3.000 €.
- Equipment with hardware VXI Agilent and software VSA, necessary for analysing the electromagnetic spectrum. Its price is about 5.000 €.

[32] The exact value for a distance of 22 cm has been calculated with the basic propagation losses equation taking -34 dBm as reference as it's measured at the edge of the antenna.

- Microsoft Office 365 licence, necessary for the development of the report. Available for 7 € per month, and it will be used during 5 months.
- Computer ASUS A52J version K52JU, necessary for the realization of the application and the report. It costs 600€.
- Student work, necessary for the realization of the Bachelor Thesis. It has been supposed an expenditure of 40 €/hour and 360 hours worked in total, equivalent to 12 credits according to Bachelor Thesis regulations.
- Professor work, necessary to guide the student with the Bachelor Thesis. It has been supposed an expenditure of 60 €/hour and 60 worked hours in total, equivalent to 12 credits according to Bachelor Thesis regulations.
- Indirect costs, like internet access, electric expense, etc. It has been supposed an expenditure of 100 €/month during 5 months.

The costs[33] are mentioned in the table below:

Material	Costs
LabVIEW Student Edition licence	0 €
NI USRP 2920	3.000 €
Equipment with hardware VXI Agilent and software VSA	5.000 €
Microsoft Office 365 licence	35 €
Computer ASUS A52J version K52JU	600 €
Student work	14.400 €
Professor work	3.600 €
Indirect costs	500 €
TOTAL	27.135 €

Table 7/Bachelor Thesis's budget

[33] Taxes included.

Anexos

Anexo 1: Resumen (castellano)

Este trabajo fin de grado consiste en la realización de una aplicación mediante Software Defined Radio que inhibe la señal del sistema de comunicaciones móviles LTE. El hecho de trabajar con comunicaciones móviles supone una motivación tanto en lo profesional como en lo académico, ya que son una actividad económica puntera en nuestra sociedad y es la rama que más me ha gustado del Grado en Ingeniería en Tecnologías de Telecomunicaciones.

Los inhibidores tienen multitud de utilidades, aunque su uso quedará limitado dentro del marco legal a las actividades relacionadas con la seguridad pública, la defensa nacional, la seguridad del estado y las actividades del Estado en el ámbito del Derecho Penal.

El objetivo será realizar una aplicación que consiga dejar sin señal LTE a los terminales de una operadora específica (pero válida para todas) dentro del radio de inhibición minimizando la relación entre la potencia que recibe el móvil de la operadora y la que recibe de la aplicación, o lo que es lo mismo, consiguiendo el máximo radio de inhibición minimizando la potencia transmitida por la aplicación.

La duración de este trabajo fin de grado será de 145 días, repartidos en distintas actividades tal y como se muestra en la siguiente tabla:

Tarea	Inicio	Duración (días)
Adjudicación del Trabajo Fin de Grado	0	1
Búsqueda de información	1	3
Estudio teórico	4	20
Aprendizaje de LabVIEW	24	4
Desarrollo de la aplicación	28	30
Realización de pruebas	58	20
Mejoras	78	10
Redacción de la memoria	88	30
Revisión de la memoria	118	15
Entrega de la memoria	133	1
Preparación de la presentación	134	10
Defensa del trabajo	144	1

Tabla 8/Planificación

El diagrama de Gantt correspondiente a esta planificación es el siguiente:

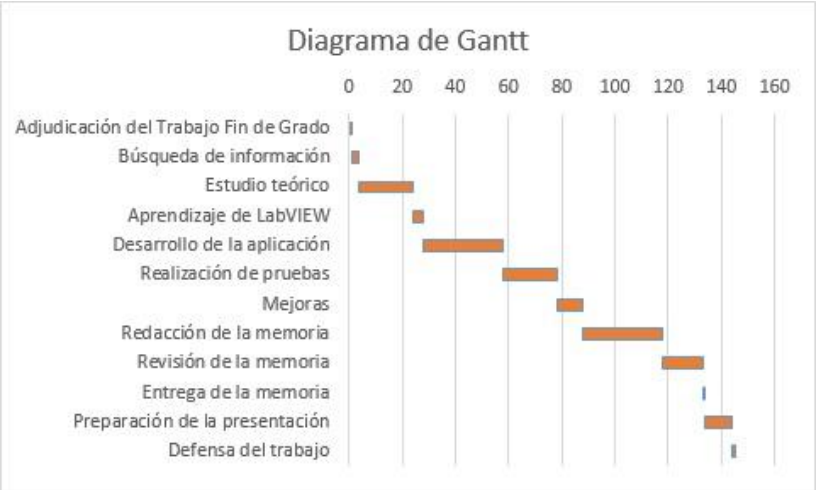


Ilustración 32/Diagrama de Gantt

Actualmente el sistema LTE tiene distintas vulnerabilidades, ya que podemos inhabilitar la comunicación interfiriendo únicamente alguno de sus canales como los que siguen: PDSCH, PUSCH, PCFICH, PUCCH, PBCH. Nosotros optaremos por inhabilitar la comunicación transmitiendo unas señales de sincronización (PSS y SSS) aleatorias tal y como se explica en [5].

Para producir nuestro ataque es necesario que transmitamos la forma de trama de LTE en el enlace de bajada y las señales de sincronización correctamente mapeadas en la trama. La trama tiene una duración de 10 ms y se divide en 10 subtramas. Cada subtrama se divide a su vez en 2 slots. La estructura de trama que utiliza LTE usando FDD es la siguiente:

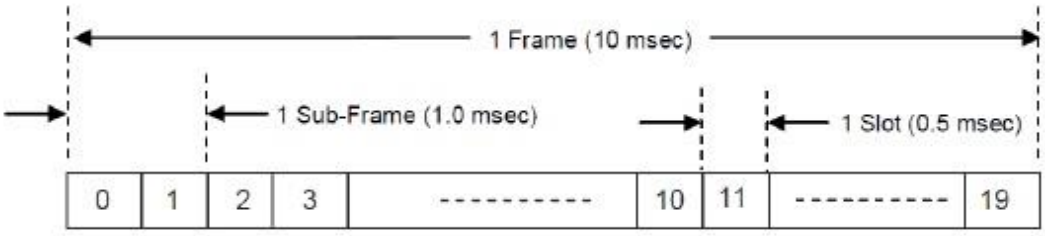


Ilustración 33/Estructura de trama

Cada trama está compuesta por 20 slots de 0,5 ms. La estructura del slot dependerá del tamaño del prefijo cíclico, ya que puede ser normal o extendido. El prefijo cíclico se utiliza como banda de guarda entre los símbolos OFDMA para que no se pierda ortogonalidad entre ellos. En nuestro caso usaremos un prefijo cíclico normal, ya que es el más utilizado.

La estructura del slot para un prefijo cíclico normal será la siguiente:

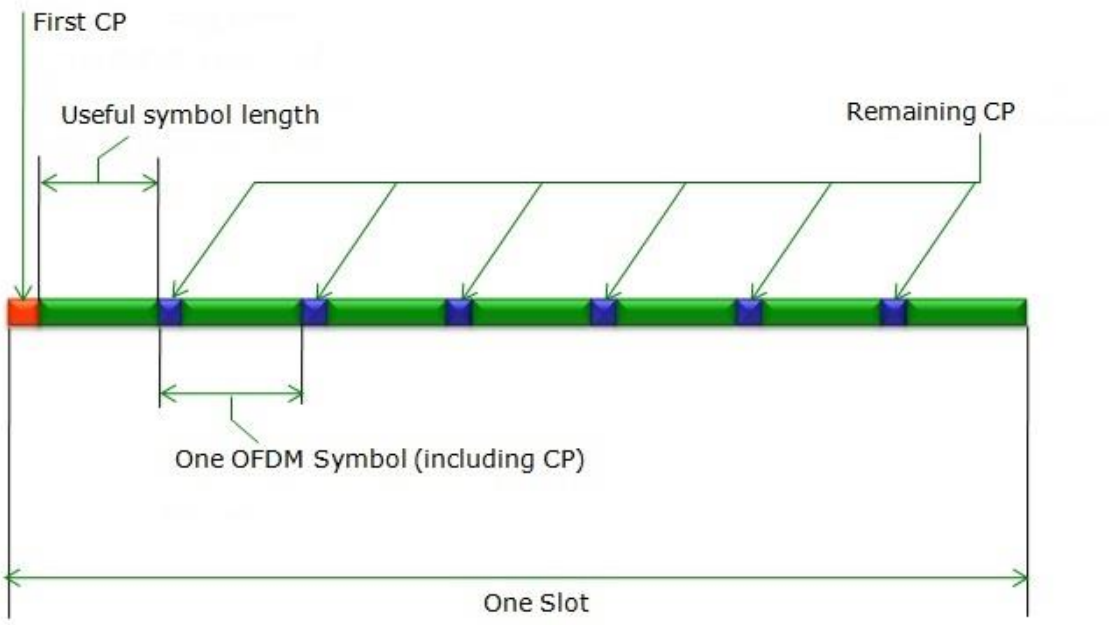


Ilustración 34/Estructura de un slot

Como se observa en la imagen, un slot contendrá 7 símbolos OFDMA, y cada símbolo irá precedido por un prefijo cíclico. Los canales se mapean en la trama como se muestra en la siguiente imagen:

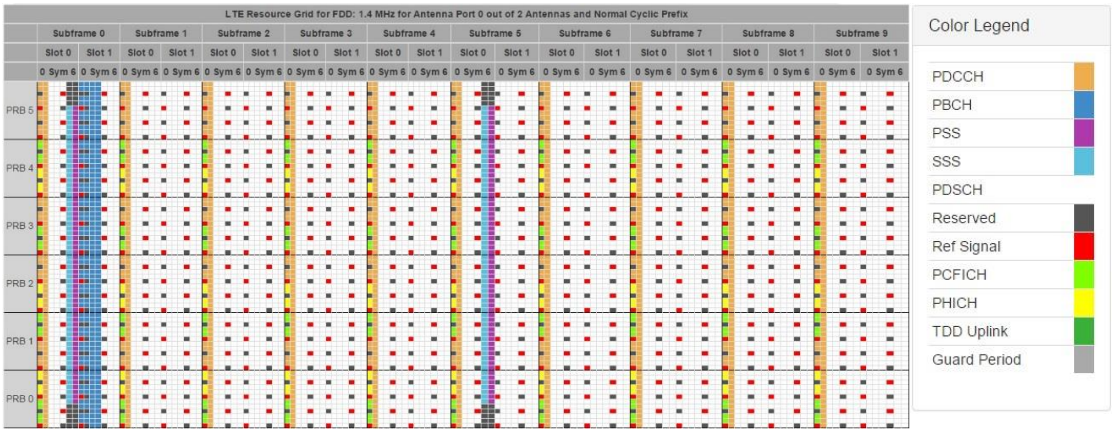


Ilustración 35/Trama con canales y señales físicas

Tal como se indica, la PSS se transmitirá en el séptimo símbolo de los slot 1 y 11 y la SSS en el sexto símbolo de los slot 1 y 11, aunque previo al mapeo será necesario hacer la IFFT a las dos señales.

Tanto la PSS como la SSS tienen una longitud de 62 elementos. Se rellenarán con 33 ceros a cada lado hasta tener un tamaño de 128 y así realizar la IFFT de tamaño 128.

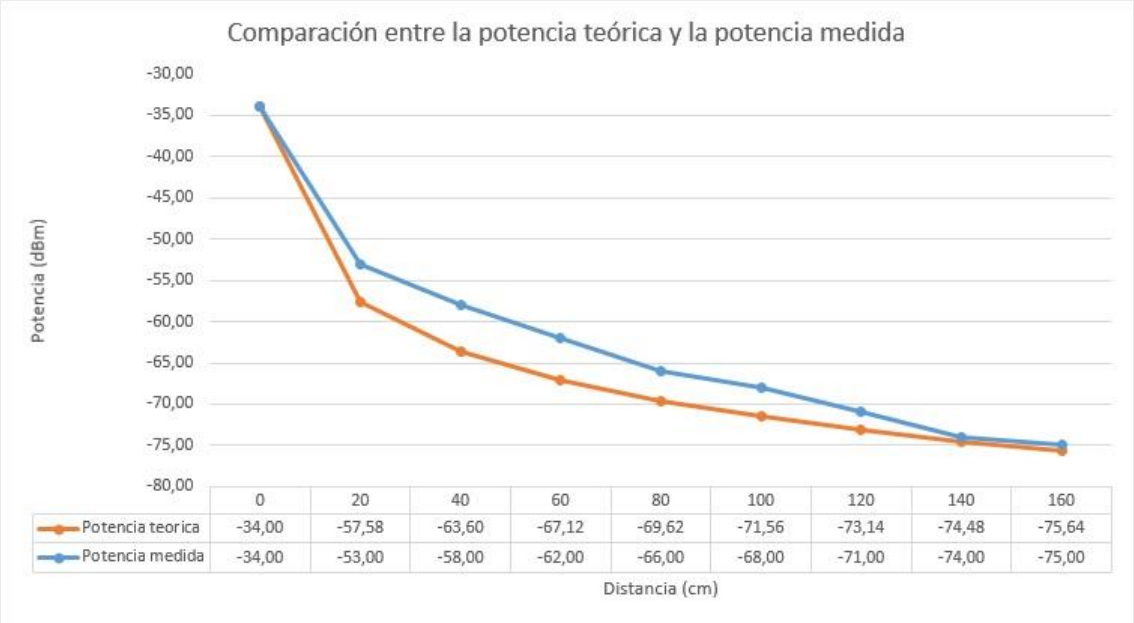
Previo a la realización de la IFFT será necesario sustituir los 64 primeros elementos por los segundos, y viceversa. Una vez realizada la IFFT se mapearán las señales y se transmitirá la trama continuamente. El resto de los elementos de la trama serán ceros modulados.

Tras la realización de varias pruebas con distintos terminales y para todas las operadoras podemos decir que nuestro inhibidor ha sido un éxito, ya que conseguimos inhibir en todos los casos y con buenos resultados.

Nuestro dispositivo tiene una potencia de transmisión en el borde de la antena de -34 dBm. Hemos medido la potencia trasmitida por el dispositivo para distintos radios de inhibición y la hemos comparado con la potencia teórica que debería llegar a esas distancias teniendo en cuenta las pérdidas básicas de propagación:

$$L_{bf}(dB) = 32{,}45 + 20\log f(MHz) + 20\log d(km)$$

El resultado es el siguiente:



	0	20	40	60	80	100	120	140	160
Potencia teorica	-34,00	-57,58	-63,60	-67,12	-69,62	-71,56	-73,14	-74,48	-75,64
Potencia medida	-34,00	-53,00	-58,00	-62,00	-66,00	-68,00	-71,00	-74,00	-75,00

Ilustración 36/Comparación entre potencia teórica y medida

Como se aprecia en la imagen, la potencia transmitida medida es muy parecida a la potencia transmitida teórica. Su diferencia de potencia, que alcanza los 5 dB, puede ser debida a las interferencias producidas en la sala.

La potencia recibida por Vodafone son -61 dBm. Para esta operadora y un terminal categoría 4 obtenemos 22 cm de radio. La potencia que nosotros medimos en ese punto aproximadamente es de -53 dBm, y la de Vodafone es de -61 dBm. Por tanto podemos decir que para inhibir necesitamos interferir la señal original en más de 8dB.

No obstante, si hacemos la misma apreciación para el valor de potencia teórico en ese punto, -58,40 dBm, que es más exacto ya que está libre de interferencias, podemos determinar que tan sólo es necesario interferir la señal en más de 2,6 dB.

Este es un resultado muy positivo en cuanto a la eficiencia de nuestro dispositivo, ya que los inhibidores actuales necesitan interferir en más de 30 dB la señal original.

Para la realización de este trabajo fin de grado hemos realizado el siguiente presupuesto:

Material	Coste
Licencia LabVIEW Student Edition	0 €
NI USRP 2920	3.000 €
Equipo con hardware VXI Agilent y software VSA	5.000 €
Licencia de Microsoft Office 365	35 €
Ordenador ASUS A52J versión K52JU	600 €
Trabajo del alumno	14.400 €
Trabajo del profesor	3.600 €
Costes indirectos	500 €
TOTAL	27.135 €

Tabla 9/Presupuesto

Anexo 2: Introducción (castellano)

1.1 Motivación y objetivo

Actualmente las comunicaciones son el pilar de la sociedad en que vivimos. Gracias a ellas sabemos lo que está ocurriendo en cualquier lugar del mundo al instante o establecer fácilmente una conversación entre dos puntos del planeta, entre otras cosas.

Las comunicaciones móviles son las más usadas hoy en día, ya que no sólo permiten el tráfico de voz, sino que también se puede acceder a Internet a gran velocidad. Aunque son un bien para nuestra sociedad, un mal uso de ellas puede ser bastante perjudicial. Es por ello que existen situaciones en las que sería necesario inhabilitarlas y para ello se hace uso de los inhibidores.

Estos dispositivos emiten ondas de radio en las mismas frecuencias que las usadas para las comunicaciones móviles pero a mayor potencia, consiguiendo así interferir el canal e impedir la comunicación.

Se usa en múltiples ámbitos de la sociedad:

- Militar y civil.
- Seguridad y restricción de uso.
- Aulas, reuniones, congresos, iglesias, penitenciarias, protección antiterrorista, etc.

El Grupo de Comunicaciones de la Universidad Carlos III de Madrid ha desarrollado una patente[34] que trata sobre un inhibidor para 3G o 4G que consigue una mayor eficiencia que los existentes en el mercado actualmente. Mi trabajo será desarrollarlo para LTE mediante Software Defined Radio, haciendo uso de la herramienta de trabajo LabVIEW y el hardware NI USRP 2920.

La realización de este proyecto me ayudará a estudiar los sistemas móviles, principalmente LTE, consiguiendo que adquiera un gran nivel de comprensión sobre estos ayudándome así en mi futuro profesional. Este será el principal objetivo del trabajo, ya que me gustaría dedicarme a la investigación de los sistemas móviles.

El objetivo general de este Trabajo Fin de Grado es desarrollar una aplicación que consiga inhibir la señal de LTE en el terminal. Para ello realizaremos una aplicación que consiga dejar sin señal LTE a los terminales de una operadora específica (pero válida para todas) dentro del radio de inhibición minimizando la relación entre la potencia que recibe el móvil de la operadora y la que recibe de la aplicación, o lo que es lo mismo, consiguiendo el máximo radio de inhibición minimizando la potencia transmitida por la aplicación. Usaremos el hardware NI USRP 2920, que nos permitirá transmitir y del software LabVIEW, con el que programaremos el hardware para que realice lo que necesitemos.

[34] http://www.google.es/patents/WO2014041225A1?cl=es&hl=es

También será necesario diseñar la señal que debemos transmitir para interferir a la señal real. Para ello haremos uso de la patente y de las asignaturas troncales del Grado en Ingeniería en Tecnologías de Telecomunicación.

1.2 Estructura de la memoria

La presente memoria consta de seis capítulos principales:

- 1. Introducción. En él se desarrollan varios aspectos fundamentales como la motivación y los objetivos para realizar este trabajo, la estructura de la memoria, la planificación seguida en la realización del trabajo y el marco que regula el dispositivo realizado.
- 2. Estado del arte. Se comparan los inhibidores existentes con la propuesta que se desarrolla.
- 3. Telefonía móvil. Se repasan las tecnologías de telefonía móvil que han existido hasta LTE, ayudando así a comprender mejor este moderno sistema de comunicación móvil para voz y datos.
- 4. Aspectos teóricos de LTE. En este capítulo se expondrán todos los conocimientos necesarios para llevar a cabo el desarrollo de nuestro dispositivo.
- 5. Descripción de la aplicación. Se explica cómo se ha desarrollado la aplicación desde el punto de vista teórico y la interfaz gráfica.
- 6. Conclusiones. En este capítulo se exponen los resultados de las pruebas realizadas y el presupuesto que supone este Trabajo Fin de Grado.

1.3 Planificación

En la siguiente tabla se muestra la planificación seguida a lo largo del proyecto:

Tarea	Inicio	Duración (días)
Adjudicación del Trabajo Fin de Grado	0	1
Búsqueda de información	1	3
Estudio teórico	4	20
Aprendizaje de LabVIEW	24	4
Desarrollo de la aplicación	28	30
Realización de pruebas	58	20
Mejoras	78	10
Redacción de la memoria	88	30
Revisión de la memoria	118	15
Entrega de la memoria	133	1

Tarea	Inicio	Duración (días)
Preparación de la presentación	134	10
Defensa del trabajo	144	1

Tabla 10/Planificación

Como se aprecia, la duración total del proyecto es de 145 días. El diagrama de Gantt correspondiente es el siguiente:

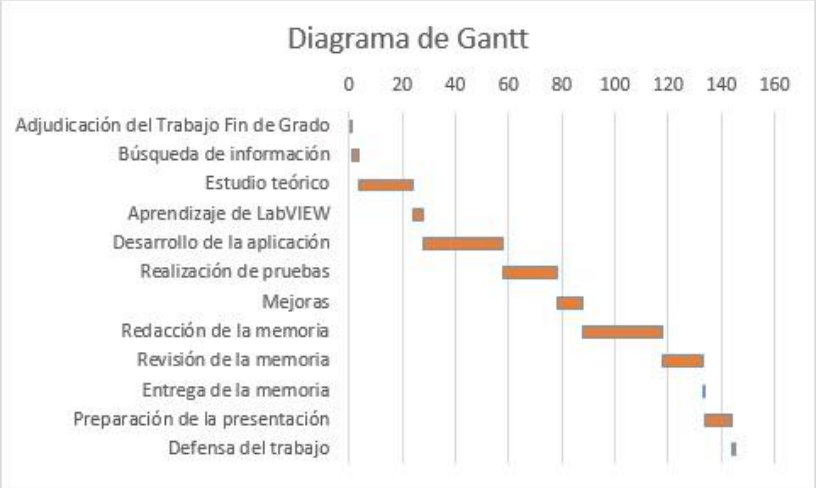


Ilustración 37/Diagrama de Gantt

1.4 Marco regulador

Aunque el sector de las telecomunicaciones y las tecnologías de la información está ampliamente regulado, no existe una ley general específica sobre los inhibidores de frecuencia. Por ello, la Comisaría General de Seguridad Ciudadana del Cuerpo Nacional de Policía realizó un informe[35] el 16 de febrero de 2010 para establecer un marco regulador no vinculante acerca de estos dispositivos.

El informe se basa en la normativa aplicable a este tipo de cuestiones, que tal y como se expresa en el mismo es la siguiente:

- Directiva de la Comunidad Europea 99/05/CE.
- Real Decreto 1890/2000 de 20 de noviembre por el que se aprueba el procedimiento para la evaluación de la conformidad de los aparatos de telecomunicaciones.
- Informe de la Secretaría de Estado de Telecomunicaciones de fecha 28 de diciembre de 2004.
- Título VIII de la Ley 32/2003 de 3 de noviembre, General de Telecomunicaciones.

[35]http://www.policia.es/org_central/seguridad_ciudadana/unidad_central_segur_pri/i_reservada/2010/2010_009.pdf

- Decisión de la Comisión de 6 de abril de 2000 relativa al establecimiento de la clasificación inicial de los equipos radioeléctricos y equipos terminales de telecomunicación y los identificadores asociados.
- Decisión de la Comisión de 26 de julio de 2002 por la que se crea un Grupo de política del espectro radioeléctrico.
- Decisión nº 676/2002/CE del Parlamento Europeo y del Consejo sobre un marco regulador de la política del espectro radioeléctrico en la Comunidad Europea.

El TCAM (Comité de Vigilancia del Mercado y evaluación de la conformidad en materia de Telecomunicaciones) de la Comisión Europea ha acordado que el uso de estos dispositivos no está autorizado, así como la venta, pudiendo llegar a sancionar a los que incumplan la normativa con multas de entre 500.000 y 20 millones de Euros.

Además, los inhibidores de frecuencia por el simple hecho de usar el espectro radioeléctrico deberán cumplir la Directiva 99/05/CE.

No obstante, las actividades relacionadas con la seguridad pública, la defensa nacional, la seguridad del estado y las actividades del Estado en el ámbito del Derecho Penal estarán autorizadas a su uso, quedando exentas de la aplicación de esta normativa.

Anexo 3: Conclusiones (castellano)

6.1 Pruebas y resultados

Como ya hemos comentado a lo largo de esta memoria, el objetivo de nuestra aplicación es claro: dejar sin servicio LTE los terminales conectados a una operadora en concreto. Para inhibir más de una operadora al mismo tiempo, será necesario conectar tantos NI USRP 2920 como operadoras queramos dejar sin servicio. En cualquier caso, las pruebas que nosotros realizaremos se centrarán en inhibir una sola operadora.

Realizamos pruebas para distintas operadoras y terminales, resultando todas exitosas.

Tenemos un radio de inhibición entre 15 cm y 1,5 m, dependiendo de la operadora, ya que cada portadora llega con distinta potencia. Para aumentarlo probamos combinando dos SSS aleatorias, de forma que aumenta la correlación de la señal y puede ser más efectiva porque nosotros no conocemos la SSS original del eNodeB.

El resultado no es positivo; para el mismo terminal y misma operadora obteníamos 22 cm de radio de inhibición con una SSS aleatoria y con la combinación de dos SSS aleatorias obtenemos un radio de 8 cm.

Parecía que todo era un éxito hasta que probamos un terminal LTE Samsung Galaxy Note 4, que seguía disponiendo de conexión bajo el radio de inhibición. Esto es debido a que el terminal no usa las señales de sincronización para mantener la conexión, sino que las almacena en su memoria. Sólo las utiliza para establecer la conexión. Por ello probaremos a conectar el terminal a LTE bajo el radio de inhibición, ya que para establecer la conexión si es estrictamente necesario usar las señales de sincronización.

Efectivamente, el terminal es incapaz de conectarse a LTE bajo el radio de inhibición, pero sí es capaz de mantener la conexión si ya estaba establecida anteriormente.

Por tanto podemos afirmar que nuestra aplicación inhibe en todos los casos, si bien no siempre con la misma efectividad ya que intervienen muchos factores.

6.2 Eficiencia

Para comprobar la eficiencia de nuestro inhibidor debemos medir la potencia[36] transmitida en el borde del radio para distintas longitudes de radio y compararla con la potencia transmitida teórica en cada punto según la ecuación de pérdidas básicas de propagación:

$$L_{bf}(dB) = 32{,}45 + 20\log f(MHz) + 20\log d(km)$$

[36] Todas las medidas de potencia están realizadas para un ancho de banda de 1,4 MHz. Para las medidas de potencia de transmisión del inhibidor se ha utilizado 1800 MHz como frecuencia de portadora.

Haciendo uso de esta fórmula calcularemos la potencia teórica transmitida tomando como referencia la potencia transmitida medida en el borde de la antena, -34 dBm. En el siguiente gráfico podemos ver la comparación entre la potencia medida y la teórica:

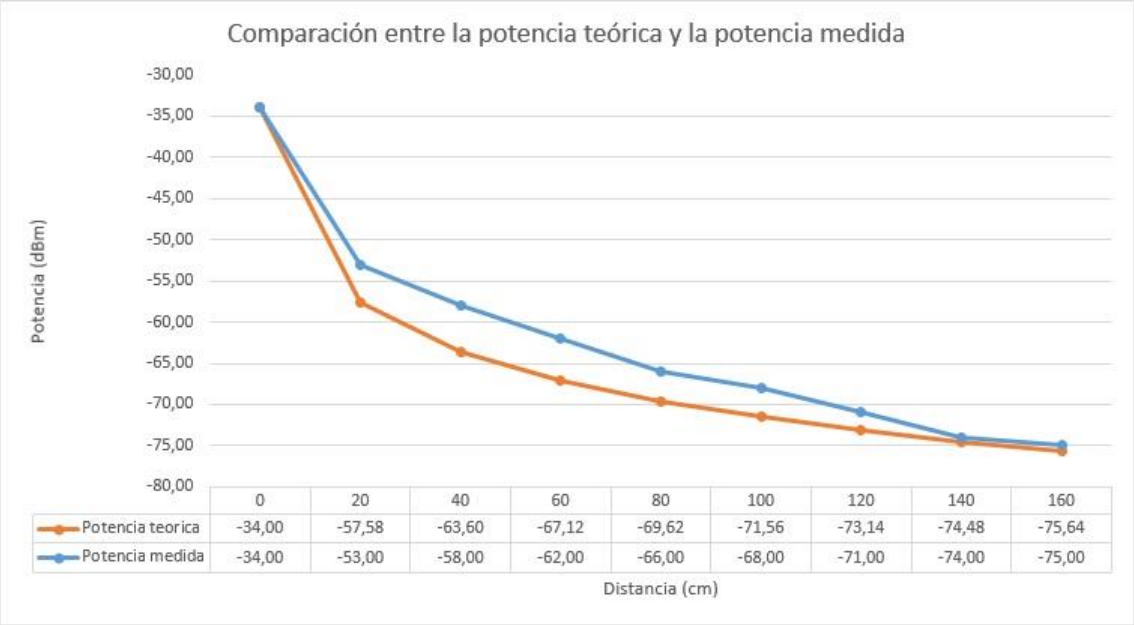


Ilustración 38/Comparación entre potencia teórica y medida

Como se observa, la potencia medida es bastante similar a la teórica, lo que apunta a que nuestros resultados son correctos. En ocasiones se llega a una diferencia de potencia de hasta 5 dB que puede ser debida a las interferencias producidas en la sala donde se han tomado las medidas.

La potencia recibida por cada operadora es la siguiente:

Operadora	Potencia
Movistar	-83 dBm
Vodafone	-61 dBm
Yoigo	-72 dBm
Orange	-54 dBm

Tabla 11/Potencia de los operadores

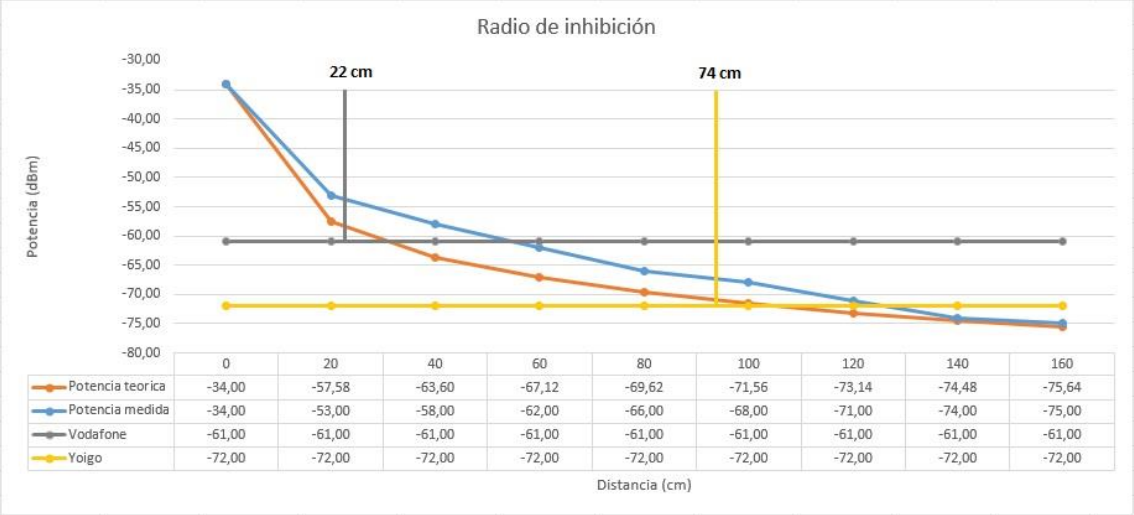
Para el caso de Vodafone obtenemos un radio de inhibición de 22 cm. La potencia que nosotros medimos en ese punto aproximadamente[37] es de -53 dBm, y la de Vodafone es de -61 dBm. Por tanto podemos decir que para inhibir necesitamos interferir la señal original en más de 8dB.

[37] Utilizamos la potencia medida a una distancia de 20 cm ya que es la más aproximada a 22 cm.

No obstante, si hacemos la misma apreciación para el valor de potencia teórico[38] en ese punto, -58,40 dBm, que es más exacto ya que está libre de interferencias, podemos determinar que tan sólo es necesario interferir la señal en más de 2,6 dB.

El caso de Yoigo es parecido, ya que tenemos un radio de inhibición de 74 cm. La potencia medida en ese punto (80 cm) es de -66 dBm y la de Yoigo es de -72 dBm, por lo que necesitamos interferir la señal original en más de 6 dB. Si hacemos la comparación con el valor de potencia teórico, -68,94 dBm, necesitaríamos interferir la señal original en más de 3 dB.

En la siguiente imagen podemos ver estos datos contrastados con los valores de potencia teóricos y medidos:



	0	20	40	60	80	100	120	140	160
Potencia teorica	-34,00	-57,58	-63,60	-67,12	-69,62	-71,56	-73,14	-74,48	-75,64
Potencia medida	-34,00	-53,00	-58,00	-62,00	-66,00	-68,00	-71,00	-74,00	-75,00
Vodafone	-61,00	-61,00	-61,00	-61,00	-61,00	-61,00	-61,00	-61,00	-61,00
Yoigo	-72,00	-72,00	-72,00	-72,00	-72,00	-72,00	-72,00	-72,00	-72,00

Ilustración 39/Radio de inhibición

Este es un resultado muy positivo en cuanto a la eficiencia de nuestro dispositivo, ya que los inhibidores actuales necesitan interferir en más de 30 dB la señal original.

6.3 Presupuesto

El material necesario para llevar a cabo este trabajo fin de grado se detalla a continuación:

- Licencia de LabVIEW Student Edition, necesaria para la implementación de la aplicación. Es una versión gratuita por utilizarse para la realización de un trabajo fin de grado.
- NI USRP 2920, necesario para la realización de la aplicación. Su precio oscila los 3.000 €.
- Equipo con hardware VXI Agilent y software VSA, necesario para analizar el espectro electromagnético. Su precio total oscila los 5.000 €.
- Licencia de Microsoft Office 365, necesaria para el desarrollo de la memoria. Está disponible por 7 € al mes, y la usaremos durante 5 meses.

[38] Valor exacto para 22 cm de distancia calculado con la ecuación de pérdidas básicas de propagación usando como referencia -34 dBm medidos en el borde de la antena.

- Ordenador ASUS A52J versión K52JU, necesario para la realización de la aplicación y de la memoria. Tiene un precio de 600 €.
- Trabajo del alumno, necesario para la realización del trabajo fin de grado. Suponemos un gasto de 40 €/hora y 360 horas trabajadas en total, que es el equivalente a 12 créditos según la normativa del trabajo fin de grado.
- Trabajo del profesor, necesario para orientar al alumno en el trabajo fin de grado. Suponemos un gasto de 60 €/hora y 60 horas trabajadas en total, que es el equivalente a 12 créditos según la normativa del trabajo fin de grado.
- Costes indirectos, como el acceso a internet, gasto eléctrico, etc. Estimamos un gasto de 100 €/mes a lo largo de los 5 meses.

Si presentamos los gastos mencionados en una tabla quedaría el siguiente presupuesto[39]:

Material	Coste
Licencia LabVIEW Student Edition	0 €
NI USRP 2920	3.000 €
Equipo con hardware VXI Agilent y software VSA	5.000 €
Licencia de Microsoft Office 365	35 €
Ordenador ASUS A52J versión K52JU	600 €
Trabajo del alumno	14.400 €
Trabajo del profesor	3.600 €
Costes indirectos	500 €
TOTAL	27.135 €

Tabla 12/Presupuesto

[39] Impuestos incluidos.

Bibliografía

[1] "José María Hernando Rábanos, Comunicaciones Móviles, 2ª edición"

[2] "José Manuel Huidobro Moya, Comunicaciones Móviles"

[3] "José María Hernando Rábanos, Transmisión por radio, 3ª edición."

[4] "Stefania Sesia, Issam Toufik, Matthew Baker, LTE – The UMTS Long Term Evolution, Second Edition"

[5] "Ana García Armada, Víctor P. Gil Jiménez, Método y dispositivo para la inhibición de señales de telefonía móvil. http://www.google.es/patents/WO2014041225A1?cl=es&hl=es"

[6] "3GPP, ETSI TS 136 211 V9.1.0 (2010-04) http://www.etsi.org/deliver/etsi_ts/136200_136299/136211/09.01.00_60/ts_136211v090100p.pdf"

[7] "3GPP, ETSI TS 136 212 V9.4.0 (2011-10) http://www.etsi.org/deliver/etsi_TS/136200_136299/136212/09.04.00_60/ts_136212v090400p.pdf"

[8] "3GPP, ETSI TS 136 302 V9.3.1 (2012-01) http://www.etsi.org/deliver/etsi_ts/136300_136399/136302/09.03.01_60/ts_136302v090301p.pdf"

[9] "3GPP, ETSI TS 136 300 V9.10.0 (2013-02) http://www.etsi.org/deliver/etsi_TS/136300_136399/136300/09.10.00_60/ts_136300v091000p.pdf"

[10] "3GPP, ETSI TS 136 101 V9.21.0 (2015-02) http://www.etsi.org/deliver/etsi_ts/136100_136199/136101/09.21.00_60/ts_136101v092100p.pdf"

[11] "Víctor P. Gil Jiménez, Tema 4: Redes de Comunicaciones Móviles Terrestres, GTT Sistemas de Telecomunicación (2013/2014)"

[12] "Dirección general de la policía y de la guardia civil, Informe UCSP Nº: 2010/009 http://www.policia.es/org_central/seguridad_ciudadana/unidad_central_segur_pri/i_reservada/2010/2010_009.pdf"

[13] "Mavit Lorenzo, Miguel Armando, Sistemas OFDM http://bibing.us.es/proyectos/abreproy/11479/fichero/2-Sistemas+OFDM.pdf"

[14] "Universidad Carlos III de Madrid, Oficina de patentes http://www.uc3m.es/ss/Satellite/UC3MInstitucional/es/TextoMixta/1371206656681/Oficina_de_patentes"

[15] "Martín Diomedes Bravo Obando, Diseño e implementación de un prototipo inhibidor de señales de celular para un salón de clases http://journalusco.edu.co/index.php/IngenieriayRegion/article/view/385/393"

[16] "Marc Lichtman, Jeffrey H. Reed, Vulnerability of LTE to Hostile Interference http://arxiv.org/pdf/1312.3681v2.pdf"

[17] "Venta de inhibidores por Internet http://www.projammers.com/es/inhibidores-de-frecuencia/inhibidores-segun-bandas-frecuencia/inhibidores-3g-y-4g/"

[18] "Normativa TFG UC3M, http://portal.uc3m.es/portal/page/portal/organizacion/secret_general/normativa/estudiantes/estudios_grado/NormativaTrabajoFindeGrad_definitiva.pdf"

[19] "NIECOM COMUNICACIONES S:L., Procedimiento dinámico de control y conmutación de antenas, para la inhibición de señales de telefonía móvil, http://www.oepm.es/pdf/ES/0000/000/02/21/13/ES-2211305_B1.pdf"

[20] "Venta de NI USRP 2920 por Internet http://sine.ni.com/nips/cds/view/p/lang/es/nid/212995"

[21] "Licencia de Microsoft Office https://products.office.com/es-es/office-365-personal"

[22] "Telesystem innovations, LTE in a Nutshell, http://www.tsiwireless.com/docs/whitepapers/LTE%20in%20a%20Nutshell%20-%20Physical%20Layer.pdf"

[23] "Dushantha N. K. Jayakody, Leonardo O. Iheme, Erhan A. Ince, Coded QPSK-OFDM for Data Transmission over Fading Channels http://www.researchgate.net/publication/230821010_Coded_QPSK-OFDM_for_Data_Transmission_over_Fading_Channels"